

This is a continuation of SJC Hearing from File
DOCUMENTS-OCA-2 FDPS page 193

103

Follow up Questions from Senator Leahy

128. Section 203(a) of the PATRIOT Act authorized criminal investigators to disclose grand jury information to the CIA and other intelligence agencies, but required post-disclosure notification to the court. Can you give us a sense of how the notice requirement in section 203(a) has worked in practice? Has it interfered with information-sharing in any significant way, and if so, how?

ANSWER: We do not believe that the notice requirement in section 203(a) has significantly interfered with information sharing. The notice requirement in section 203(a) accords with long-standing grand jury practice, pursuant to which government attorneys file notices with the court reporting certain disclosures of grand jury information. Because it is limited to grand jury information, the notice requirement in section 203(a) is not especially onerous. For these reasons, the Administration is not seeking the repeal of the notice requirement in section 203(a)

141. Section 217 of the PATRIOT Act allows computer service providers that are victims of attacks by computer trespassers to authorize persons acting under color of law to monitor trespassers on their computer systems in a narrow class of cases. If Congress renews section 217, would the Department agree to report on its use on an annual basis, and if not, why?

ANSWER: Because reporting requirements necessarily reduce the time available to prosecutors and investigators to pursue cases, the Department does not support imposition of a new reporting requirement with respect to this provision. Service providers have long been able to monitor their own networks to guard against harm to their "rights or property" (18 U.S.C. 2511(2)(a)(i)), as well as to disclose to law enforcement the resulting evidence of wrongdoing. See, e.g., *United States v. Harvey*, 540 F.2d 1345, 1352 (8th Cir. 1976). Such disclosures have never been subject to a reporting requirement, and the Department does not believe it any more necessary to report the common-sense measures taken under the authority of Section 217 to protect the rights and privacy of victim computer owners and their users.

143. Was notice provided to Portland attorney Brandon Mayfield pursuant to this provision, and if so, on what date?

ANSWER: By letter dated March 24, 2005, the Department of Justice voluntarily notified Mr. Mayfield that he was the target of physical searches of his residence and of electronic surveillance and other physical searches authorized pursuant to FISA.

44

EFF Section 215-713

When the PATRIOT Act was being negotiated, your predecessor sought the authority to detain aliens suspected of terrorism indefinitely without charge. Section 412 of the Act, while not as broad as the Justice Department requested, gives the executive branch considerable authority to hold such aliens.

147. Has this provision ever been used?

ANSWER: No.

148. If not, why not?

ANSWER: As of yet, there has not been a suitable case for invoking the provision.

149. If this provision has never been used, do you believe it should be retained?

ANSWER: The provision should be retained because it is reasonably conceivable that it could be needed in the future. If the release of an alien would present national security concerns, the government needs the statutory authority to detain the alien. Indeed, for this reason, Congress should more clearly establish the government's detention authority. Section 412 suffers from three potential infirmities. First, the statute does not expressly authorize post-order detention. Second, an alien could argue that detention is impermissible unless the Attorney General certifies that the alien is a danger before the alien is taken into custody, 8 U.S.C. § 1226a(a)(1), and before removal proceedings begin, 8 U.S.C. § 1226a(a)(5). Third, one could contend that classified information may not be used in these proceedings. Although the Department does not find these arguments convincing, there is no reason to run the risk that a court might be persuaded. When an alien is a terrorist or presents other national security concerns, the statute should eliminate any doubt that the government is equipped to protect the American people. Congress should eliminate these potential problems by clarifying the government's detention authority. Moreover, Congress should also establish that the government has the authority to detain beyond six months an alien who presents a danger to the community or to foreign policy. In the wake of *Zadvydas v. Davis*, 533 U.S. 678 (2001) and *Clark v. Suarez-Martinez*, 125 S.Ct. 716 (2005), such express authority is necessary to protect the American public from harm. Finally, it is worth noting that detention decisions under Section 412 are judicially reviewable, so if the government does decide to invoke Section 412, the alien will have access to federal court review.

150. In your written answer to a question (#16) that I submitted following your confirmation hearing, you stated: "The material witness statute should not be used as a broad preventative detention law, to hold suspects indefinitely while investigating them without filing charges. Nevertheless, the fact that the person who is detained as a material witness also is a suspect in the underlying criminal investigation should not prevent the Government from attempting to obtain the

person's testimony through lawful means." Suppose that a suspect detained as a material witness invokes his Fifth Amendment right not to be a witness against himself. If the Government chooses not to grant him immunity for his testimony, can the Government continue to hold him as a material witness, with no reasonable prospect that this will enable the government to obtain and preserve his testimony?

ANSWER: There are adequate checks and balances in the system to prevent abuse. Most notably, the detention of any material witness must be ordered by a judicial officer, and a detention order is subject to review or appeal within the judiciary branch. It is not up to the Department to unilaterally decide to detain a person as a material witness *at all*, much less indefinitely. Under 18 U.S.C. § 3144, a judicial officer must determine whether the witness's testimony is material in a criminal proceeding, and whether it is impracticable to secure the person's presence by subpoena. Only then can the court order that the material witness be detained pending his testimony.

At the detention hearing, the material witness may be represented by an attorney, and counsel will be appointed if the witness cannot afford one. The material witness has the ability to challenge the basis for detention at the detention hearing itself, and may seek a review of the detention hearing under § 3145(b), or may file an appeal of an order of detention under § 3145(c). If a court finds that the person does not meet the criteria of § 3144, the court may not detain that person as a material witness.

Once a court orders detention, a material witness still has an avenue to challenge his detention. Under the provisions of § 3142(f), the detention hearing may be reopened, either before or after a determination by the judicial officer, if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that the information has a material bearing on the reasons for detention.

To fully address the hypothetical scenario you describe would require more facts to give a definitive answer, but generally, the material witness could be detained up to the time that he appears before the grand jury and invokes the Fifth Amendment. At that time, if we were not willing to grant the witness immunity, we would go back to the court and inform the court of the circumstances. If, in fact, the witness did not have any further testimony material to the proceeding that could be given, there would most likely be no basis for further detention.

Finally, it remains the Department's position that, even though in certain circumstances it may be proper to seek a material witness warrant for a suspect in the underlying investigation, the material witness statute should not be used to hold suspects indefinitely while investigating them without filing charges. That is not the purpose of the material witness statute.

151. In your same response to question #16, you declined to comment on some proposed changes to the material witness statute, saying that you "would have to

consult with the experts in the Department of Justice to assess the impact the amendments would have on the administration of justice.” Now that you have had an opportunity to consult with DOJ experts, would you support amending 18 U.S.C. §3144 to limit the “reasonable period of time” that a witness may be detained to a time certain (e.g., no more than 3 days, consistent with the requirements of 18 U.S.C. §3142(f)(2)) or, alternatively, to require that the witness’s testimony be taken, whether by grand jury or deposition, at the first available opportunity?

ANSWER: Because the detention of material witnesses is dealt with under § 3142, the provisions of § 3142(f) to which you refer already apply in the case of the detention of a material witness. Under that section, a material witness is entitled to a *detention hearing* before a judicial officer immediately on the witness’s first appearance before a judicial officer, unless either the witness or the government seeks a continuance. Except for good cause, on a motion from the government, the hearing may be continued for no more than three days, and on a motion from the witness, the hearing may be continued no more than five days.

At the hearing, the judicial officer will determine whether the individual’s testimony is material to a criminal proceeding, and whether it is impracticable to secure the presence of the witness by subpoena. The material witness is afforded an opportunity to testify, to present witnesses, to cross-examine witnesses and to present information by proffer or otherwise. The hearing may be reopened before or after a determination by the judicial officer, if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that has a material bearing on the issue whether there are conditions of release that will reasonably assure the appearance of the person.

We would oppose any specific time limitation on the detention of material witnesses subsequent to a court order, for a number of reasons. First, and most significantly, districts vary significantly in how and when their grand juries convene. In smaller districts, where grand juries meet less frequently, it may be difficult to get a material witness before a grand jury in only a few days. Additionally, it is not always practical to determine how extensive a material witness’s testimony will be. Questioning in the grand jury itself is likely to reveal new lines of questioning that prosecutors may want to pursue—extending the amount of time the witness may need to be detained. Similarly, it is not always possible to determine the extent to which the material witness will be cooperative. It is not unlikely that the material witnesses may be evasive or obstructive in the grand jury—again, extending the possible time of their detention. Putting a rigid time frame on the total time of detention would hamstring federal prosecutors—especially those from less populated districts—and could result in the loss of valuable testimony.

Two questions (#21B and #22) that I submitted to you following your confirmation hearing pertained to the federal death penalty. To both questions, you responded

that you would study the issues “carefully” if confirmed. Please answer those questions now.

160. Will you continue the policy, instituted by former Attorney General Ashcroft, of requiring that U.S. Attorneys clear all plea bargains with you? Why or why not?

ANSWER: The goal of the death penalty protocol is the fair, consistent, and even-handed application of the federal capital sentencing laws nationwide, irrespective of personal or community based bias for or against the death penalty. Clearly, that goal could be undermined by disparate practices regarding the circumstances that justify the withdrawal of a death notice. Accordingly, we consider continuation of this practice essential to the fair and consistent application of the capital sentencing laws.

161. Will you restore the pre-2001 version of section 9-10.070 of the U.S. Attorney’s Manual, which protected the interests of non-death penalty states like Vermont by ensuring that the absence of a state death penalty statute did not by itself establish a sufficient federal interest for capital prosecution? Why or why not?

ANSWER: The protocol in effect from January 27, 1995, to June 6, 2001, provided: “In states where the imposition of the death penalty is not authorized by law, the fact that the maximum federal death penalty is insufficient, standing alone, to show a more substantial interest in federal prosecution.” The elimination of this provision has not resulted in a significant, if any, increase in the number of death penalty prosecutions in non-death penalty states. For a homicide to be prosecuted in federal court, there must be a corresponding federal offense, and the decision whether to prosecute the crime in state or in federal court is usually mutual and founded on a variety of factors. While the elimination of this provision has not had a significant impact on federal charging practices, it could come into play in an appropriate case. The Department is not going to reinstate the identified provision.

163. Following your confirmation hearing, I asked you about a number of immigration cases, including (in question #28) whether you would retain the controversial “automatic stay” policy that was used for the “special interest” immigration detainees who were detained in the wake of the 9/11 attacks and, if so, why the traditional standard for release on bond in immigration proceedings – risk of flight or danger to the community – was inadequate. You replied that you had not had the opportunity to familiarize yourself with the details of immigration procedures, adding, “I look forward to looking into both of these issues if confirmed.” Have you looked into these issues and if so, would you please respond now to the questions?

ANSWER: The automatic stay regulation does not change the "traditional standard" for release on bond in immigration proceedings. See 8 C.F.R. § 1003.19(i)(2). Rather, it provides an orderly process for reconciling conflicting custody decisions by the Department of Homeland Security and an immigration judge, and is supported by the substantial policy considerations described when the regulation was published. See 63 Fed. Reg. 27441, 27447 (May 19, 1998); 66 Fed. Reg. 54909 (Oct. 31, 2001). As explained, "[t]his stay is a limited measure and is limited in time -- it only applies where the Service determines that it is necessary to invoke the special stay procedure pending appeal, and the stay only remains in place until the Board [of Immigration Appeals] has had the opportunity to consider the matter." 66 Fed. Reg. at 54910.

The process by which the Attorney General and the Secretary of the Department of Homeland Security exercise their discretion under INA § 236(a) with respect to whether an alien should be detained during removal proceedings involves multiple administrative components. Under the regulations, Immigration and Customs Enforcement makes the initial custody decision in each case -- that is, whether to keep the alien in detention pending completion of the removal proceedings, or whether to release the alien on bond or other appropriate conditions. The alien may appeal this determination to an immigration judge. 8 C.F.R. § 236.1(d)(1). That decision may in turn be appealed to the Board. 8 C.F.R. § 236.1(d)(3). See generally *Pisciotta v. Ashcroft*, 311 F. Supp.2d 445, 455 (D. N.J. 2004) ("consistent with the reasoning in [*Kim v. Demore*, this Court finds that the automatic stay provision effecting the ongoing detention of Petitioner, a criminal alien in pending removal proceedings, is constitutionally permissible"). The automatic stay regulation preserves the status quo while the Board, and on occasion the Attorney General, finally adjudicates the issue. Accordingly, we intend to retain the regulation.

At the April 5 hearing, I asked about an e-mail released to the ACLU in response to its FOIA litigation. The e-mail is dated May 10, 2004, addressed to T.J. Harrington at the FBI, and contains the subject line, "Instructions to GTMO interrogators" (copy enclosed). Over the past six months, the Department has released the same e-mail in three different redacted versions. When asked about the e-mails at the hearing, you stated that you "would like to study the e-mail and talk to the people involved" in redacting the information before answering any questions. As you know, there is a presumption of disclosure under the FOIA, but agencies may withhold information pursuant to exemptions and exclusions in the statute, such as information properly classified, or protected by the Privacy Act. The three versions of the e-mail described above were significantly different from one another in what was redacted and what was released. Much of the information that was eventually released does not fit squarely within a FOIA exemption, suggesting that it should have been released pursuant to the ACLU's original request.

164. Please explain the process followed by the Department and its components in reviewing documents for release under FOIA.

ANSWER: Requests for records under the Freedom of Information Act (FOIA) are initially processed by the Department components that possess the records. If the component does not produce all of the responsive records or redacts information from those records pursuant to FOIA's statutory exemptions, then the requestor is advised of his or her administrative appeal rights. Administrative appeals are adjudicated by the Department's Office of Information and Privacy (OIP) and often result in the release of additional text. A requestor may file suit in U.S. District Court if he or she is dissatisfied with the results of this process. Alternatively, requesters may file suit if the Department component does not respond to the request within the statutory time frame, as the ACLU chose to do in connection with the document request that included the FBI e-mail, dated May 10, 2004, that was described in your question.

165. When documents that originated with the FBI are sought by a FOIA requestor, is it the FBI or DOJ that ultimately determines what information can be released?

ANSWER: As indicated above, each Department component (including the FBI) makes the initial determination in response to FOIA requests for its own records. Thereafter, the administrative appeal process conducted by OIP may result in the additional release and, in some cases, further determinations to release may occur in the litigation process.

166. How could the FOIA process, with its well-defined exemptions, lead the Department or the FBI to release three different versions of the same document?

ANSWER: As indicated above, the originating component may initially release the document in one redacted form and a subsequent review by OIP, as part of an administrative appeal process, may result in a partial reversal of the component and a second release with reduced redactions.

A non-identical duplicate of the FBI document, dated May 10, 2004, (Bates 1373) was initially released by the FBI between September 15 and October 15, 2004, in accordance with the schedule for processing 1,388 pages, which the Court imposed in the ACLU litigation. A non-identical duplicate is, in this instance, an e-mail that contains the same information embedded in a different e-mail. The FBI processed the other version of the same document (Bates 2709) in November without the same time constraints, resulting in a different judgment regarding the release of information and, hence, reduced redactions.

In March, OIP was asked to review the document (Bates 2709) as if it were the subject of an administrative appeal and, in that process, the FBI agreed to release additional text, which had previously been withheld to protect privacy interests and deliberative process. This revised version was provided to Senators Levin and Lieberman, as well as the ACLU on March 18, 2005. As the cover letter to the Senators noted, a small amount of text remained redacted because it implicated the interests of the

Department of Defense (DOD) and, in accordance with established third-agency practice, there was an obligation to consult with DOD prior to making a decision on that text. On or about April 6, 2005, a fourth version of the document was disclosed to the Senators and the ACLU, which restored that text based upon the DOD review.

167. In discussing Defense Department interrogations that used coercive techniques, the document states that, "results obtained from these interrogations were suspect at best." The words "suspect at best" were redacted in the first two versions of the document that were released, but not redacted in the final version that was released to Senator Levin. Please explain why "suspect at best" was initially redacted.

ANSWER: The FBI cited FOIA exemption (b)(5) in the margin corresponding to the "suspect at best" redaction, which pertains to "inter-agency and intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." See 5 U.S.C. 552(b)(5). Exemption (b)(5) has been construed by the courts to exempt records that are normally privileged in the civil discovery process and is most commonly invoked to protect information relating to an agency's deliberative process. The "suspect at best" text was restored by the OIP review and was included in the version that was provided to Senators Levin and Lieberman with the Department's letter, dated March 18, 2005, and again, following the DOD consultation, in the version released on April 6, 2005.

168. I recently re-introduced the Restoration of Freedom of Information Act, S.622. The text of the bill is identical to the text of a White-House-endorsed compromise reached in the summer of 2002 regarding the protection of critical infrastructure information. During your confirmation process, I asked you (in question #39) whether you would support my bill. You replied that you did not have great familiarity with the issue, but would review the legislation if you were confirmed and work with me on the issue. Having had an opportunity to review the Restoration of Freedom of Information Act, do you support it and if not, why not?

ANSWER: As emphasized in our response to previous question #39, it is important to safeguard critical infrastructure information that is submitted to the federal government by the private sector for homeland security-related purposes, while at the same time also protecting the interests of openness in government. And we recognize that attempting to achieve this balance as best as possible is at the heart of the proposed legislation to which you refer. This is a matter that is of particular concern to the Department of Homeland Security, given its unique responsibilities in this subject area. As mentioned in our previous response that the Department of Homeland Security was then in the process of moving from an interim rule to a final one in its regulations on this subject, with further relevant information to be obtained during that process, and we are advised that this still remains the case. We are also advised that the Department of Homeland Security has not yet taken a position on this legislative proposal in this Congress, let alone communicated

a position on behalf of the executive branch. So it is most appropriate for the Department of Justice to defer consideration of this proposed legislation at this time. However, we can reiterate that, as the Justice Department stated in its most recent annual report to Congress on the FOIA (dated April 1, 2005), we look forward to continuing to work together with the Congress, in a constructive partnership based upon our mutual interests in sound FOIA administration, on all matters pertaining to the Act.

169. I also asked you after your confirmation hearing (in question #38) whether you would, if confirmed, continue Attorney General Ashcroft's FOIA policy or revert to a policy presumption based upon disclosure. You said you had not had the opportunity to review the Ashcroft FOIA policy, but promised that, "if confirmed, I would undertake an examination of the Department's policies and practices concerning FOIA disclosures." Have you undertaken such an examination and, if so, would you please respond now to the question?

ANSWER: The federal government's overall Freedom of Information Act ("the Act") policy certainly is an important matter, and in the Attorney General's prior position as Counsel to the President he had occasion to become generally familiar with this subject, perhaps more so than most incoming Attorneys General. Consequently, the Attorney General has readily become comfortable with the Department's overall policies for FOIA administration, including the Ashcroft FOIA policy memorandum of October 12, 2001, to which you refer. Insofar as your question asks whether the Attorney General anticipates that the Department will "revert to a policy presumption based upon disclosure," which might appear to be somewhat confusing, we can only reply that information disclosure always has been and remains the dominant objective of the Act, both law and policy. To reiterate what the Department stated in its most recent report to Congress on this subject on April 1, 2005: "I can assure you of the Department of Justice's firm commitment to the Freedom of Information Act, as amended by the Electronic Freedom of Information Act Amendments of 1996, and to its faithful implementation."

170. Shortly after you were confirmed as Attorney General, you gave a speech in which you discussed some of your priorities. You stated, "As we battle crime, we must also defend the rights of crime victims and assist them in their recovery." You then noted the Administration's support of a Victims Rights Constitutional Amendment, which you called, "a priority for the President and a priority for me." Yet just a few weeks earlier, President Bush sent Congress a budget that proposed raiding the Crime Victims Fund of an estimated \$1.2 billion. I find it hard to reconcile your rhetoric with your policies. Did the proposal to rescind the Fund originate at the Justice Department or at the White House? Do you support the President's proposal to rescind the Crime Victims Fund at the end of FY06?

ANSWER: The Administration has consistently supported the rights of crime victims and continues to recognize the need to empower and support those who provide vital services to crime victims. The President's Fiscal Year 2006 budget requests \$650 million to support the Crime Victims Fund. This is \$30 million more than Congress had enacted in Fiscal Year 2005. The Department recognizes that government-wide cuts in programs have been proposed and supports the President's Budget.

The funding source for the Crime Victims Fund, which provides crucial services and assistance to victims, will continue to be criminal fines, forfeited bail bonds, penalties and special assessments, and gifts, bequests or donations from private entities. The rationale for the rescission of remaining funds is that because the balances are controlled by obligation limitations only, the balances "rollover" and become available again every year -- a never ending offset. In essence, it's the same offset year after year. Rescinding the balances prevents them from rolling over on an annual basis, and is a more straight forward approach to budgeting.

Please be assured the Administration, and the Attorney General personally, remain committed to supporting services and assistance for crime victims and their families, and to efforts to improve the treatment of crime victims in the justice system.

173. In 1999, the President signed into law the Treasury and General Government Appropriations Act for Fiscal Year 2000 (P.L. 106-58), which created the National Intellectual Property Law Enforcement Coordination Council. One of the co-chairs of NIPLECC is the Assistant Attorney General of the Criminal Division of the Department of Justice. The President has nominated Alice Fisher to replace AAG Christopher Wray. What steps, if any, are being taken to ensure that during the transition the important work of NIPLECC does not literally get lost in the shuffle?

ANSWER: The protection of intellectual property rights continues to be an important focus of the Department, both through the aggressive investigation and prosecution of criminal intellectual property violations, and through the renewed work of the Department's Task Force on Intellectual Property. The Administration, through the Strategy Targeting Organized Piracy (or "STOP!"), has made intellectual property enforcement a top interagency priority. Given this emphasis on intellectual property protection, the joint work of the NIPLECC agencies has taken on a new importance and even has extended beyond the formal NIPLECC process. AAG Wray's replacement will be fully briefed on all aspects of intellectual property enforcement and all aspects of interagency coordination on these issues, including NIPLECC. Given the importance of intellectual property to the Administration and to the Department, there is no chance that the task of coordinating enforcement will be overlooked in the transition period.

174. Protecting America's artists and innovators through strong intellectual property enforcement is vital to ensuring that the United States continues to be the world leader in intellectual property. In that effort coordination is critical. Please describe some of the Department's recent efforts in working with NIPLECC to coordinate enforcement efforts.

ANSWER: The Department continues to work closely with the other agencies in NIPLECC to ensure that the intellectual property rights of U.S. citizens and corporations are enforced through using the full range of appropriate civil, administrative and criminal mechanisms, both domestically and abroad. The Department's domestic criminal enforcement efforts benefit from referrals of IP violations through the Commerce Department's website at www.StopFakes.gov, and the joint FBI/ICE National Intellectual Property Rights Coordination Center website at <http://www.ice.gov/graphics/cornerstone/ipr/>. Internationally, the Department has continued to assist foreign nations in building the criminal law enforcement capacity to protect intellectual property. The Department's success in international capacity building would not be possible without the financial and logistical assistance of the State Department, and the subject-matter expertise of other NIPLECC agencies including the U.S. Patent and Trademark Office, DHS Customs and Border Protection and Immigration and Customs Enforcement. The Department will continue to work with all the NIPLECC agencies to ensure a coordinated response to intellectual property crime by the United States Government.



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 20, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find attached responses to questions for the record posed to Attorney General Gonzales following his appearance before the Senate Committee on the Judiciary on April 5, 2005. The subject of the hearing was, "Oversight of the USA PATRIOT Act". With this letter we are pleased to transmit the remaining portion of unclassified responses to questions posed to the Attorney General. This transmittal supplements our earlier letter, dated June 29, 2005.

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Handwritten signature of William E. Moschella in cursive.
William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Hearing Before the Senate Judiciary Committee On
"OVERSIGHT OF THE USA PATRIOT ACT"
Witness: Attorney General Alberto Gonzales
April 5, 2005

Follow up Questions from Chairman Specter

1. When "roving" or "multi-point" surveillance authority under FISA was debated on the Senate floor, Senator Feingold offered an amendment that would have imported an "ascertainment" requirement from the criminal wiretap law (Title III) and added it to FISA. His amendment would have required the person implementing a roving FISA order to ascertain the presence of the target before conducting the surveillance. A similar requirement has been proposed as part of the SAFE Act. Given that a multi-point FISA wiretap could conceivably cover several different devices, should Congress import some type of ascertainment requirement to reduce the potential interception of innocent third-party communications?

ANSWER: No. The "ascertainment" requirement contained in the criminal wiretap statute applies to the interception of oral communications, such as through bugging and not interception of wire or electronic communications, such as telephone calls. The statute states interception of oral communication "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." 18 U.S.C. § 2518(12).

In the context of wire or electronic communications, the criminal wiretap statute imposes a more lenient standard allowing surveillance to be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." 18 U.S.C. § 2518(11)(b)(iv).

The SAFE Act's ascertainment requirement thus would make it more difficult for investigators to conduct roving wiretaps against international terrorists and spies than it is to conduct such wiretaps against drug dealers and organized crime figures.

Moreover, the Foreign Intelligence Surveillance Act (FISA), contains safeguards to ensure that the government does not intrude on the privacy of innocent Americans. These safeguards include the requirements that: all targets of roving wiretap orders must be identified or described in the order of the FISA Court; the FISA Court must find probable cause to believe the target is an agent of a foreign power, such as a terrorist or a spy, to issue a roving wiretap order; the order will be issued only if the FISA Court determines the target may thwart surveillance; and all roving surveillance orders must include court-approved minimization procedures that limit the acquisition, retention, and

dissemination of information and communications involving United States persons. In light of these protections, and the fact that foreign governments and international terrorist groups regularly utilize counter-surveillance techniques that are more sophisticated than ordinary criminals, we believe the roving provisions of FISA must be flexible to allow the United States to successfully monitor the activities of foreign powers and their agents and must not contain an ascertainment requirement.

Finally, please see the enclosed documents regarding section 206 of the USA PATRIOT Act and the Department's views letter on the SAFE Act. (Enclosures 1 & 2)

At the hearing, Attorney General Gonzales said that Section 207, by extending the duration of FISA surveillance of non-U.S. persons, had saved the Department "nearly 60,000 attorney hours." At the same time, however, the Attorney General was unprepared to discuss the length of time it takes for the Department to process a FISA surveillance order.

2. How long, on average, does it take to obtain a first-time surveillance order under FISA?

ANSWER: It is difficult to answer this question because the Department historically has not tracked electronically the interval between the time an FBI agent in the field first begins to formulate a request for FISA collection until the time the order is signed by the FISA court. The estimated number of attorney hours saved that was referenced in the Attorney General's testimony was only intended to reflect the number of hours saved at Main Justice, and was not an estimate of the number of hours saved at the FBI.

3. What factors contribute to the total time needed to obtain such an order?

ANSWER: A variety of factors can affect the time it takes to obtain an order for surveillance or search under FISA. The main factors that determine the time it takes to process a request for FISA coverage are the priority assigned to the request by the Intelligence Community and the strength of the factual predication underlying the request. Urgent requests that meet the criteria and requirements of FISA are handled as emergency or expedited matters. Lower priority requests, as well as those that require additional investigation or other steps to fulfill the requirements of the Act, are handled as promptly as possible. Additional factors that contribute to the time it takes to process a FISA request include the certification and approval requirements of the Act as well as the fact that most FBI requests originate from FBI field offices around the country but are attested to by FBI headquarters agents in Washington, D.C., creating a need for additional procedures to verify the factual accuracy of the request before filing.

4. Have the changes made by Section 207—which require the Department to renew such orders less frequently—led to a reduction in the time needed to obtain an order?

ANSWER: Yes. The changes have allowed the Department to no longer spend time on repeated renewals every 90 days for orders for surveillance of certain non-U.S. person cases after those targets have been initially approved for such intelligence collection by a FISA Court judge, as well as repeated renewals of physical search applications every 45 days for all agents of foreign powers. These changes have permitted more resources to be dedicated to the careful processing of U.S. person cases and the processing of increased volumes of other FISA requests.

5. Are the most exigent cases being processed more rapidly?

ANSWER: Yes. As noted in the answer to question number three above, urgent requests that meet the criteria and requirements of FISA are handled as emergency or expedited matters.

At the hearing, Attorney General Gonzales said the FISA court has “granted the department’s request for a 215 order 35 times as of March 30, 2005.” One of the concerns raised by critics of Section 215 is that it does not require individualized suspicion—that is, the records sought by the government need not relate directly to a specific investigative target.

11. Can you report in an unclassified response whether any of the 35 orders issued under Section 215 have any been for a large category of documents—such as a list of the members of a group or organization?

ANSWER: The answer to this question is classified and was provided to the Committee under separate, classified cover on July 21, 2005.

12. Have any of the 35 orders been issued for “tangible things” other than business records? If so, can you generally describe those “tangible things”?

ANSWER: The tangible things sought in each instance were records kept by an entity that maintains records in the ordinary course of their operations. We provided additional information responsive to this question under separate, classified cover on July 21, 2005.

15. Without discussing the specifics of classified cases, can you report whether Section 215 has allowed the FBI to obtain records that it could not otherwise have obtained using preexisting legal tools?

ANSWER: Although it is possible that some of the records obtained could have been obtained pursuant to federal grand jury subpoenas or National Security Letters, we believe that section 215 was the appropriate tool to use in these circumstances in light of the underlying nature and purpose of the investigations at issue.

16. For electronic surveillance under FISA, there are minimization requirements. Are there similar limits on the Government's ability to retain or disseminate documents regarding innocent third parties obtained under Section 215?

ANSWER: All applications for electronic surveillance and physical search under FISA must include proposed minimization procedures that are approved by the Attorney General. The FISA Court reviews those procedures to determine whether they meet the definition of such procedures under the Act, and then orders the government to follow them in implementing the surveillance or search. Limits on the FBI's use of materials collected pursuant to section 215 orders are contained in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection that were promulgated on October 31, 2003.

17. Have any materials obtained via Section 215 been used in subsequent criminal proceedings?

ANSWER: Not to our knowledge.

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 amended the FISA definition of an "agent of a foreign power" to include a foreign national who is preparing for, or engaging in, international terrorism. This amendment is subject to the sunset provision of section 224 of the USA PATRIOT Act.

20. Can you report in an unclassified response whether this new authority—to treat so-called "Lone Wolf" terrorists as agents of a foreign power—[has] been used since its adoption late last year?

ANSWER: The answer to this question is classified and was provided to the Committee under separate, classified cover on July 21, 2005.

21. Would you agree that it may be difficult to assess the impact of this provision by the sunset date, December 31, 2005?

ANSWER: The Department strongly supports repealing the sunset on the "Lone Wolf" provision. If an individual is engaging or preparing to engage in international terrorism, investigators should be able to obtain FISA surveillance of that individual. The "Lone Wolf" provision allows FISA to be used to investigate only non-United States persons who are engaged in international terrorism or are preparing to engage in international terrorism, even if they are not known to be affiliated with an international terrorist group. Prior to the amendment, the FBI could not obtain a FISA surveillance order of an international terrorist unless it could establish a connection to a foreign organization. The "Lone Wolf" provision therefore closed a dangerous gap in our ability to protect against terrorism, as even a single foreign terrorist with a chemical, biological, or radiological weapon, or an airplane could inflict terrible damage on this country. The threat lone wolf terrorists pose will not cease to exist at the end of 2005. Moreover, the provision protects civil liberties of Americans, as it applies only to non-U.S. persons; applies only to international and not domestic terrorism; and requires court authorization and the use of significant restrictions on the collection, retention, and dissemination of information acquired through surveillance.

Follow up Questions from Senator Kennedy

34. During the April 6, 2005 Judiciary Committee hearing, Director Mueller testified that people "higher in the hierarchy in the FBI" had conversations with Defense Department personnel regarding the abuse of detainees witnessed by FBI agents at Guantanamo Bay. Director Mueller testified that the FBI sent a letter to the Defense Department reflecting concerns about the abuse.

Please identify the FBI and Defense Department Personnel that participated in the conversations.

ANSWER: As indicated in the FBI's 7/14/04 letter to DoD, provided in response to Question 35, below, Mr. Marion Bowman, then-Deputy General Counsel for the FBI's National Security Law Branch and subsequently FBI Senior Counsel for National Security Affairs, discussed the treatment of GTMO detainees with DoD Deputy General Counsel (DGC) Del'Orto and Deputy General Counsel (Intelligence) Dietz. In addition, FBI Counterterrorism Division Deputy Assistant Director (DAD) T.J. Harrington has been interviewed on two occasions by DoD officials. The FBI has cooperated with other DoD investigative efforts, and both DAD Harrington and others may have discussed this matter with DoD officials on other occasions. In addition to DGC Del'Orto and DGC Dietz, Major General Geoffery Miller, Lieutenant Colonel (LTC) Jerry Phifer (GTMO officer overseeing military interrogations), LTC Diane Beaver (Staff Judge Advocate), NCIS SACs David Khurt, Blaine Thomas, and Tim James, and other more junior DoD officials were also aware of the FBI's concerns regarding the treatment of GTMO detainees.

35. Please provide a complete, un-redacted copy of the letter. If the letter, or any portion of it is classified, provide it to the appropriate full Committee staff in classified form (with notification to each office that this has been done), and immediately thereafter to each of the Committee members in redacted unclassified form, in original formats and pagination to show size and locations of redactions. Names of recipients and approval markings should not be redacted.

ANSWER: We have enclosed the FBI's 7/14/04 letter to Major General Ryder, DoD, reflecting the FBI's concerns regarding the treatment of Guantanamo (GTMO) detainees. This letter has been redacted so it may be provided in unclassified format.

The FBI provided the classified 7/14/04 letter to this Committee in response to Questions for the Record following its 5/20/04 hearing (Enclosure B to the classified response). While classified information is not redacted from that letter, it does contain minimal redactions pursuant to FOIA exemptions b(6) and b(7)(C) related to clearly unwarranted invasions of personal privacy. (Enclosure 3)

36. Please provide a complete, un-redacted copy of all Defense Department responses and FBI replies (follow the procedure described above for any classified documents).

ANSWER: DoD confirmed receipt of the FBI's 7/14/04 letter, but did not reply to it.

37. Please provide all memoranda and correspondence which provided background or support for drafting the FBI correspondence (follow the procedure described above for any classified documents).

ANSWER: The FBI provided a classified 5/30/03 electronic communication, and its attachments, to this Committee in response to Questions for the Record following its 5/20/04 hearing (Enclosure A to the classified response). Other than that 5/30/03 communication and its attachments, the FBI has located no final FBI memoranda or other correspondence responsive to this inquiry, other than earlier drafts of the 7/14/04 letter and comments on those drafts. These drafts are not provided because we have furnished to the Committee the signed 7/14/04 letter.

During your confirmation hearing, you made specific reference to the possibility of your having a role in investigating the substance of the FBI e-mails produced by the ACLU that reported interrogation abuses at Guantanamo Bay. You called the accuracy of the e-mails into question due to a claimed erroneous reference to an "Executive Order." We now know, as Director Mueller testified on April 6, 2005, that there was high level communication by the FBI expressing concern about abuses at Guantanamo Bay.

40. Are you still skeptical of the FBI reports that detainee abuses were committed at Guantanamo Bay? If so, why?

ANSWER: The FBI raised concerns about the use of aggressive interrogation methods with personnel in the Department of Defense (DoD) and the Department of Justice. We have no reason to doubt that the FBI agents accurately reported events they observed at GTMO. Whether the observed interrogation techniques had been approved and whether the military interrogator stayed within or exceeded the bounds of any authority granted are, we understand, matters that are being investigated by DoD.

The May 10, 2004 FBI e-mail which described the FBI's concerns about abuse and the ineffectiveness of the Defense Department's interrogation practices identified several Justice Department employees who participated in the relevant discussions. Among the employees identified was Alice Fisher, who has been nominated to be Assistant Attorney General for the Criminal Division.

41. Don't these circumstances reinforce the need for you to disqualify yourself from involvement in any investigation into the allegations of abuse?

ANSWER: Please see the response to question 43, below.

42. If you disagree, please explain how you could fairly and impartially conduct an investigation of this magnitude involving the Department.

ANSWER: Please see the response to question 43, below.

43. Doesn't the appearance of a conflict of interest require you to recuse yourself from any investigation that might involve Justice Department employees?

ANSWER: The Department of Justice has demonstrated its willingness to investigate aggressively those who might have violated the law in their treatment of detainees. Moreover, the FBI e-mail referred to indicates that the FBI agents were instructed to follow Bureau policy in conducting interrogations. Nothing in the e-mail or the discussions it describes suggests that the Department of Justice will not continue to conduct professional and thorough investigations in this area.

The FBI e-mail in question indicates that the FBI questioned the DoD methods of interrogation at the Guantanamo Bay military facility (GTMO)—particularly, whether the methods were effective and productive of reliable intelligence—and instructed FBI agents not to be involved in any methods of interrogation at GTMO that deviated from FBI policy. FBI policy forbids agents to attempt to obtain a statement by force, threats, or promises.

The FBI has since initiated a special inquiry into FBI agents' observations of interrogation techniques employed at the GTMO and Abu Ghraib military facilities. The Justice Department's Office of the Inspector General (OIG) requested materials from the FBI relating to this special inquiry and, after reviewing these materials, opened its own review of this matter. The OIG is examining whether any FBI staff observed or participated in non-law enforcement interrogation techniques of detainees at U.S. military detention facilities. The OIG is also reviewing whether FBI employees reported their observations of these interrogation techniques and how those reports were handled.

The Department of Justice has been responsive to referrals of alleged criminal misconduct involving detainees. As evidenced by the indictment of David Passaro, a CIA contractor alleged to have mistreated a detainee in Afghanistan, the Department of Justice has vigorously pursued allegations of criminal abuse of detainees that have been referred to the Criminal Division, regardless of the location of the alleged abuse. The Passaro investigation was launched in 2003; the matter is currently pending trial in the Eastern District of North Carolina.

Last June, then-Attorney General John Ashcroft announced the consolidation of all ongoing abuse investigations in the United States Attorney's Office for the Eastern District of Virginia (with the exception of the Passaro matter, which is venued in North Carolina). New referrals are assigned to the Eastern District of Virginia, where a special prosecution team has been formed to work on these matters. That U.S. Attorney's Office is one of our finest, staffed with experienced prosecutors who have a track record of success in complex matters involving national security, classified information, and military intelligence. The Eastern District is the home of the Pentagon and the CIA.

As the Department continues to investigate these matters, we will maintain the high standards of professional integrity that we apply to all our investigations and prosecutions. If, at any point in time, a conflict of interest arises with respect to the Attorney General or any other official in connection with our work in this area, we will take prompt action to recuse the conflicted party.

On March 11, the New York Times reported that the Pentagon is planning on reducing the number of detainees at Guantanamo by more than half. The transfers would be subject to interagency approval, including the Justice Department, and the prisoners could be turned over to Saudi Arabia, Afghanistan, and Yemen.

In January, you told this committee, that the government has "an obligation not to render someone to a country that we believe is going to torture them," and that "additional assurances", are sought from countries suspected of using torture.

44. How does the interagency approval process work?

ANSWER: The United States has no interest in detaining enemy combatants longer than necessary. The Department of Defense has established a process to review the detention of each individual it holds at Guantanamo Bay Naval Base, Cuba, to determine whether continued detention is warranted based on factors such as whether the detainee continues to pose a threat to the United States and its allies or whether a foreign government is willing to accept responsibility for ensuring, consistent with its laws, that the detainee will not continue to pose such a threat. Senior United States Government officials are involved in deciding whether to transfer a detainee. The Government makes such decisions on a case-by-case basis, taking into account factors such as the particular circumstances of the transfer, the country, and the individual concerned. The Department

of State generally has responsibility to communicate on these matters as between the United States and foreign governments. The Secretary of Defense, or his designee, ultimately approves a transfer deemed to be appropriate.

45. Aren't these transfers just exporting torture? Aren't they just renditions under a different name?

ANSWER: No. The President has recently and repeatedly reaffirmed the longstanding policy that the United States will neither commit nor condone torture; nor will it transfer individuals to countries to be tortured. Consistent with the Convention Against Torture, it is the policy of the United States not to transfer an individual to a country if the United States determines that it is more likely than not that the individual will be tortured.

46. What "additional assurances" do you seek from these other countries? How do you know they prevent torture?

ANSWER: Consistent with the Convention Against Torture, it is the policy of the United States not to transfer an individual to a country if the United States determines that it is more likely than not that the individual will be tortured. It is the policy of the United States to seek appropriate assurances, including, where appropriate, assurances that the government accepting transfer will not subject the individual to torture. The essential question in evaluating foreign government assurances is whether the appropriate United States Government officials believe it is more likely than not that the individual will be tortured in the country to which he is being transferred. As the Department of State has explained in litigation involving Guantanamo detainees, the Department of State works closely with the Department of Defense and relevant agencies to advise on the likelihood of torture in a given country, and on the adequacy and credibility of assurances obtained from a particular foreign government, prior to any transfer of a detainee from Guantanamo Bay, and recommendations by the Department of State are formulated at senior levels through a process involving Department of State officials familiar with the conditions in the countries concerned. Consistent with United States policy, in an instance in which specific concerns about torture cannot be resolved satisfactorily, the United States has in the past not, and would in the future not, transfer a detainee.

Since 9/11, the U.S. has flown 100 to 150 suspects to countries like Egypt, Saudi Arabia, Syria, and Jordan – countries that we know engage in torture. We turned over a Canadian to Syria, where he was tortured for nearly a year, until the Syrians decided that he had no ties to Al Qaeda and released him. We detained an Arab German and flew him to Afghanistan, where he was drugged, and beaten, and eventually released five months later. We captured an Arab citizen of Australia and flew him to Egypt. He says that he was given intense electric shocks, hung from metal hooks, beaten, and almost drowned. We eventually released him from Guantanamo.

47. Aren't you just turning a blind eye to torture?

ANSWER: No. The President has repeatedly affirmed that it is the policy of the United States not to transfer individuals to countries to be tortured. The United States is committed to complying with its obligations under the Convention Against Torture. Consistent with the Convention Against Torture, it is the policy of the United States not to transfer an individual to a country if the United States determines that it is more likely than not that the individual will be tortured.

The State Department's 2004 Country Reports on Human Rights practices has this to say about Saudi Arabia:

"...Authorities reportedly at times abused detainees, both citizens and foreigners. Ministry of Interior officials were responsible for most incidents of abuse of prisoners, including beatings, whippings, and sleep deprivation. In addition, there were allegations of beatings with sticks and suspension from bars by handcuffs. There were allegations that these practices were used to force confessions from prisoners."

The Human Rights Report said this about Afghanistan:

"Security forces reportedly used excessive force during their fight against Taliban and al-Qa'ida remnants, including looting, beating, and torturing of civilians Prisoners reportedly were beaten, tortured, or denied adequate food."

We know these people are likely to be tortured. Yet we still send them there.

48. How can we claim with a straight face that we are honoring our obligations under the Convention Against Torture, when we know these countries practice torture?

ANSWER: As described in the response to question 47 above, the President has repeatedly affirmed that it is the policy of the United States not to transfer individuals to countries to be tortured. The United States is committed to complying with its obligations under the Convention Against Torture. Consistent with the Convention

Against Torture, it is the policy of the United States not to transfer an individual to a country if the United States determines that it is more likely than not that the individual will be tortured. Where appropriate, the United States seeks appropriate assurances, including, as the circumstances warrant, assurances that the government accepting transfer will not subject the individual to torture.

It is important to note that the Country Reports on Human Rights Practices are relevant but not necessarily dispositive in assessing whether it is more likely than not that a particular individual will be tortured by a receiving foreign government. It should be borne in mind that, for example, the Country Reports may describe problems that are confined to a particular facility or component of a government, may reflect certain types of fact patterns that are not applicable to the situation at hand, or may raise concerns that can be appropriately addressed through assurances deemed acceptable by the United States from the receiving government and, in appropriate cases, monitoring mechanisms.

Of all the concerns raised about the PATRIOT Act, the absolute prohibition on anyone who receives a FISA order or a National Security Letter from talking about it to anyone – ever – is the scariest, the most abusive. The gag order puts an individual completely at the mercy of the Administration. The Supreme Court has bluntly said that “a state of war is not a blank check for the President when it comes to the rights of the nation’s citizens.” Coercing silence about government conduct is going too far.

49. Why shouldn’t the FBI, at least be required to distinguish between cases where a gag order is necessary or isn’t necessary? Orders can be used against anyone, even if the person is not suspected of espionage or a crime. Why shouldn’t they be able to consult a lawyer or tell their spouse it’s happening?

ANSWER: 18 U.S.C. § 2709(c) prohibits wire and electronic communication service providers and their officers, employees, and agents from disclosing that the FBI has sought or obtained access to information or records pursuant to a National Security Letter. As explained in our answer to Question 51 below, disclosure of such information would identify the targets of foreign intelligence and counter-terrorism investigations, could provide terrorists and foreign intelligence agents with critical information about the scope and direction of our government’s investigatory activities, and could allow them to evade ongoing investigations and formulate counter-measures. The fact that the recipient or subject of the NSL is not suspected of involvement in terrorism or foreign intelligence does not eliminate these risks. However, 18 U.S.C. 2709(c) does not prohibit the recipient of an NSL from consulting a lawyer. The language of Section 2709(c) contemplates that NSLs may be disclosed by a communication service provider to its “officer[s], employee[s], or agent[s],” and a communication service provider’s counsel is one of its agents. The existing statutory language permits a recipient of an NSL to consult counsel regarding its legal rights and obligations in responding to the NSL, as the Department of Justice has argued in litigation.

Similarly, the Department of Justice has taken the position in litigation that a recipient of a section 215 order may consult with an attorney and may challenge the order. As the Attorney General testified, the Department supports amending section 215 to clarify that a recipient may disclose receipt to legal counsel and that a recipient could seek judicial review of the production request.

Nor do we agree that NSLs or section 215 orders "can be used against anyone." An NSL can be issued only in an authorized National Security investigation, which may cover foreign intelligence related to a non-U.S. person, international terrorism, or espionage. Further, NSLs can only be issued in narrow, statutorily authorized circumstances, such as to obtain toll billing records. A non-disclosure requirement is standard and sensible in sensitive international terrorism or espionage investigations. A section 215 order is similarly limited in scope: it can only be used (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, much less "against anyone." Finally, the use of section 215 is subject to congressional oversight; every six months, the Attorney General must "fully inform" Congress on how it has been implemented.

50. How is anyone supposed to know they can ask for help if they've been told, "Don't tell anyone about this."

ANSWER: Please see the response to question 49, above.

51. Regardless of the justification, why should the gag order be perpetual? Shouldn't an innocent person be able to challenge future use of the information, or future seizures if no justification existed?

ANSWER: FISA orders deal with highly sensitive matters related to national security, namely terrorist activities and espionage. It is imperative that secrecy be maintained with regard to such matters. As noted above, if a recipient of a request for business records believes the request is inappropriate, they have the right to consult counsel and challenge the validity of the order in court. We would strongly oppose any provision that might result in premature notice of an ongoing investigation to a target.

The non-disclosure provision of Section 215 of the PATRIOT Act is neither novel nor remarkable. For example, Title III (electronic surveillance) and the Right to Financial Privacy Act (bank records) contain similar provisions. In a foreign intelligence or counter-terrorism investigation, the need for secrecy is manifest. There is no room for unauthorized disclosures that would undermine the investigation. As the D.C. Circuit recently explained, disclosure of this type of information would identify the targets of foreign intelligence and counter-terrorism investigations, would "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] could 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, 928-929 (D.C. Cir. 2003). Accordingly, the First Amendment does not preclude the government from imposing restrictions on the disclosure of information gained by witnesses and others as a result of participation in a counter-terrorism or foreign intelligence investigation where such restrictions are necessary to protect the integrity and efficacy of the investigation and national security. Indeed, the courts have upheld permanent restrictions on disclosure of information obtained in connection with judicial proceedings where an adequate justification exists. For example, the courts routinely impose protective orders in civil litigation which permanently prohibit disclosure of confidential information obtained in connection with the proceeding, a practice which was upheld by the Supreme Court in Seattle Times v. Rhinehart, 467 U.S. 20 (1984). Similarly, the courts have upheld permanent restrictions on disclosure of information presented to grand juries. Butterworth v. Smith, 496 U.S. 624, 633 (1990) (permanent bar on disclosure of information witness already knew before testifying was invalid but permanent prohibition on disclosure of testimony by other witnesses who might otherwise “be deterred from presenting testimony due to fears of retribution” remained enforceable); Hoffman-Pugh v. Keenan, 338 F.3d 1136 (10th Cir. 2003) (upholding Colorado statute which permanently prohibited grand jury witnesses from disclosing what transpired before the grand jury). A permanent restriction is warranted in the case of foreign intelligence and counter-terrorism investigations because they are often focused on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency, rather than solving a particular crime. See United States v. United States District Court, 407 U.S. 297, 322-323 (1972). Consequently, the need for confidentiality does not cease to exist upon an indictment or conviction in a single case.

Without requiring even a minimum threshold of suspicion, the law invites abuse. A person's records ought to be free from government scrutiny unless there is enough reason to examine them.

The FBI can get the name of everyone who checked out a particular book from a library or bought it at a book store, if it claims the information is, needed “to protect against international terrorism or clandestine intelligence activities.” Power like that is far too broad. Our last Attorney General didn't hesitate to say that anyone who questioned security policy was aiding the enemy.

52. Why shouldn't the FBI be required to demonstrate that someone is suspicious before we open up the most private aspects of their life to government intrusion?

ANSWER: Under section 215, requiring a showing that the individual whose records may be obtained is a foreign power or agent of a foreign power would hinder investigators' abilities at the early stages of an investigation. Suppose, for example, investigators sought to eliminate a potential target from suspicion and could do so through examination of business records. Almost by definition, investigators would not be able to show that the records pertained to a foreign agent or power, if the purpose was to narrow the field of potential suspects. Law enforcement may also investigate individuals who are in contact with a known terrorist or spy in order to determine whether the individual is also a terrorist or spy. Finally, valuable information relating to an ongoing investigation may be obtained from these records even though investigators may not be able to link an individual directly at such an early stage in the investigation.

Section 215 also contains a number of safeguards that make it more protective of privacy than the authorities for ordinary grand jury subpoenas. An Article III judge must explicitly authorize the use of section 215 through a court order. Prior to authorization, the court must find that the requested records are sought for (and thus relevant to) "an authorized investigation ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2). Section 215 also expressly protects First Amendment rights, providing that the FBI cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." Finally, the use of section 215 is subject to congressional oversight; every six months the Attorney General must "fully inform" Congress on how it has been implemented.

Section 215 has not been used to request information from either bookstores or libraries between the passage of the PATRIOT Act and March 30, 2005. As the Attorney General testified, the reading habits of Americans are of no interest to those conducting intelligence investigations. To the contrary, historically terrorists and spies have used libraries to plan and carry out activities that threaten our national security, and we should not allow libraries to become a safe haven for terrorists.

53. Why is it harmful to the country to require that you reasonably suspect someone of being a threat before we open their lives to government scrutiny?

ANSWER: Pursuant to section 215, a judge "shall" issue an order "approving" the release of records if the judge finds that the application meets the requirements of this section. As a result, before issuing an order requiring the production of any records under section 215, a federal judge must find that the requested records are "sought for" (and thus implicitly relevant to) "an authorized investigation...to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." Therefore, we view section 215 orders as being governed by the same relevance standard that is used with respect to grand-jury subpoenas.

Moreover, section 215 contains numerous safeguards that make it more protective of individuals' privacy than grand jury subpoenas. First, it explicitly provides that the FBI cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." In addition, section 215 is used at the preliminary stages of an investigation, and can be used to clear an individual from suspicion and to determine whether far more intrusive investigatory tools are justified. If the standard were raised from relevance, investigators would be hindered at the early stages of investigations, which would have an adverse effect on our ongoing efforts to maintain an effective anti-terror campaign.

Raising the standard from relevance would make it more difficult to investigate terrorists and spies than to investigate drug dealers or bank robbers. Investigators, for example, would be denied access to records that are indisputably relevant to an international terrorism investigation simply because the records do not specifically pertain to the suspected terrorist. But information about those associated with suspected terrorists may be relevant to a terrorism investigation just as such information is relevant in criminal investigations.

54. Under the current use of Section 215 orders, do you agree that you could obtain the entire membership list of every person in a particular place of worship if someone you had suspicions about was a member of it?

ANSWER: Section 215 makes clear that the Government cannot obtain any tangible thing under that provision for an investigation of a United States person if that investigation is based solely on activities protected by the First Amendment to the Constitution of the United States. The government would not file an application seeking the information referenced in your question unless attorneys at the Justice Department's Office of Intelligence Policy and Review (OIPR) were provided a satisfactory basis for concluding that the information would be relevant to an investigation being conducted under Executive Order 12333 (or a successor order) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Such a determination would require more facts than are provided in this question. We are also confident that the FISA Court would scrutinize such a request very carefully to ensure that it met the requirements of the statute.

55. If the answer is yes – Once you have that list, couldn't you obtain the internet records of any person on it based only on the original suspicion and nothing more?

ANSWER: As stated above, section 215 makes clear that the Government cannot obtain any tangible thing under that provision for an investigation of a United States person if that investigation is based solely on activities protected by the First Amendment to the Constitution of the United States. The government would not file an application seeking the information referenced in your question unless attorneys at the Justice Department's Office of Intelligence Policy and Review (OIPR) were provided a satisfactory basis for

concluding that the information would be relevant to an investigation being conducted under Executive Order 12333 (or a successor order) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Such a determination would require more facts than are provided in this question. We are also confident that the FISA Court would scrutinize such a request very carefully to ensure that it met the requirements of the statute.

56. If the answer is no – Please explain why you think that the law as written would not permit such a demand.

ANSWER: Please see the response to question 55, above.

Follow up Questions from Senator Biden

General Gonzales, in an exchange during the hearing with Senator Feinstein concerning Section 206 of the Act, the roving FISA wiretaps section, you noted that *"we believe there is an obligation with respect to Section 206 to either identify the person by name or to provide some type of specific description about a particular individual; that the authority is to be used with respect to a specific target"*.

78. Was this a reference to language found at 50 U.S.C. 1805(c)(1)(A) requiring that your orders specify a description of the target of electronic surveillance if the target's identity is not known?

ANSWER: It was a reference to both 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A).

79. Please provide me with an explanation of the form this "description" takes, including the level of specificity the Department typically provides the FISA Court prior to obtaining a surveillance order under section 206.

ANSWER: The Department provides the FISA Court with facts and circumstances that are adequate in each instance for the FISA Court to find that there is probable cause to believe that the target of the application is a foreign power or an agent of a foreign power, and that the minimization procedures proposed in the application meet the definition of minimization procedures under the Act.

80. How many times has the Government sought to obtain a section 206 wiretap where it could not provide the known identity of the target?

ANSWER: The answer to this question is classified and was provided to the Committee under separate, classified cover on July 21, 2005.

81. The requirement in section 1805(c)(1)(A) that the government provide a "description" of the target (where the true identity is not known) is nowhere defined in FISA. Does the Justice Department believe Congress should provide a definition of "description"?

ANSWER: No. As noted above, FISA already requires that the government provide facts and circumstances that are adequate to enable the FISA Court to find that the target of the application is a foreign power or an agent of a foreign power, and that the proposed minimization procedures meet the definition of such procedures under the Act. We believe that these provisions adequately balance the need to protect the civil liberties of Americans with the need of the government to obtain timely and accurate foreign intelligence information about the activities, capabilities, plans, and intentions of foreign powers and their agents.

Section 314(a)(2)(A) of P.L. 107-108, the Intelligence Authorization Act for Fiscal Year 2002, inserted the words "if known" at the end of subsection 50 U.S.C. 1805(c)(1)(B). This change was made under the "Technical Amendments" section of the intelligence authorization bill.

82. Please describe to me how the amendment to FISA made at Section 314(a)(2)(A) of P.L. 107-108 impacts Section 206 of the Patriot Act.

ANSWER: Before the amendment, 50 U.S.C. § 1805(c)(1)(B) provided that each order approving electronic surveillance specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed." The addition of the phrase "if known" reflects Congress's recognition that in certain circumstances, such as roving surveillance authorized by section 206 of the USA PATRIOT Act, there would be instances where the order (at the time the FISA Court judge signed it) could not specify the nature and location of each of the facilities or places at which the electronic surveillance would be directed.

83. Later in your discussion with Senator Feinstein, you noted that "[g]etting to the second prong of your question about the scope and could we simply go up on phones in an entire city, because the person might be in the city, there is a limitation that we have some reasonable basis to conclude that a set of phones is either being used or is going to be used by that specific target. So I think that there is that limitation of the law as well." As you know, when the government obtains a garden variety criminal roving wiretap, pursuant to 18 U.S.C. 2518(1)(b)(iv), it may only intercept communications "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." Could you please describe the provisions in FISA which require the government to demonstrate a "reasonable basis" for believing that a certain set of phones is being used or going to be used by a target of surveillance?

ANSWER: Title 50, United States Code, section 1804(a) requires, among other things, that each FISA application must include (1) the identity, if known, or a description of the target of the electronic surveillance; (2) a statement of the facts and circumstances relied upon by the applicant to justify the belief that the target is a foreign power or an agent of a foreign power and that each of the facilities at which the electronic surveillance will be directed is being used or is about to be used by a foreign power or an agent of a foreign power; (3) a statement of the proposed minimization procedures; (4) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to surveillance; (5) a certification from a high-ranking executive branch official with national security responsibilities that the information sought through the electronic surveillance is "foreign intelligence information" (a defined term in the statute) and that such information cannot reasonably be obtained by normal investigative techniques; (6) a statement of the means by which the surveillance will be effected; and (7) whenever more than one electronic, mechanical or other surveillance device is to be

used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device. In addition, whenever the government seeks an order from the FISA Court authorizing "roving" surveillance, it must provide the court with facts adequate for the court to make a finding that the actions of the target may have the effect of thwarting the government's ability to identify a specified person whose assistance is necessary to accomplish the electronic surveillance. All of these provisions must be read together, and as such, require the government to demonstrate a "reasonable basis" for believing that the facilities in question are being used or are about to be used by a target of surveillance. Moreover, as the FISA Court of Review made clear: "... FISA as amended is constitutional because the surveillances it authorizes are reasonable." *In Re Sealed Case*, 310 F.3d 717, 746 (For. Intell. Surv. Ct. Rev. 2002).

84. Wasn't Senator Feinstein correct when she stated that "you could get a ... wiretap to listen to all the telephones in a certain area"?

ANSWER: Please see the response to question number 83, above.

85. Doesn't the change made by section 314(a)(2)(A) of P.L. 107-108 require you to describe the phone to be tapped only if facts developed by your investigators give you the ability to make such a description?

ANSWER: Yes, because in certain circumstances, such as roving surveillance authorized by section 206 of the USA PATRIOT Act, there are instances where it is not possible to specify in advance each of the facilities or places at which electronic surveillance will be directed.

86. In those circumstances, wouldn't you also have to identify the target by name or by "description"?

ANSWER: Yes.

I will approach the Patriot Act reauthorization debate the same way I considered the initial legislation: I want your criminal and terrorism investigators to have similar powers. With that principle in mind, I note that 18 U.S.C. 2518(11)(b)(ii) requires your criminal investigators to prove to a federal judge that "there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility" when attempting to secure a roving wiretap in the criminal context. FISA does not require intelligence investigators to make a showing of probable cause regarding the thwarting of interception when they attempt to secure a roving FISA tap. They have to demonstrate to the FISA Court

that the actions of the target may have the effect of thwarting the identification of a specified person, but they do not need to meet any particular standard of proof.

87. Are there fundamental differences between criminal and intelligence investigations necessitating a differing standard of proof for securing roving wiretaps?

ANSWER: The Intelligence Community confronts the most advanced and dangerous adversaries faced by the United States. Foreign powers and their agents develop and implement highly sophisticated counter-surveillance techniques that are specifically intended to thwart the foreign intelligence collection efforts of the United States. They do so in ways that exceed counter-surveillance efforts undertaken by "ordinary" criminals of even the most sophisticated variety (such as organized crime groups). As a result, we believe that the "roving" provisions of FISA must take account of this reality, and provide the Intelligence Community with the flexibility it needs to effectively address the threats that it is charged with confronting. While analogies to criminal law often provide appropriate points of comparison to assess the tools used to conduct intelligence collection, it is not always so. We believe that FISA's current roving provision is adequately tailored to the circumstances it addresses, and is therefore reasonable under the Fourth Amendment.

88. What impact would requiring intelligence investigators to make a similar showing of probable cause to the FISA Court when attempting to secure a roving FISA wiretap have on intelligence investigations?

ANSWER: Please see the response to question 87, above.

96. At last week's hearing, you stated that the Justice Department would support efforts to amend section 215 to make it similar to a federal grand jury subpoena under Rule 17 of the Federal Rules of Criminal Procedure. Specifically, you indicated that the Department would support a change in law to clarify (1) that section 215 imposes a relevance standard, and (2) that recipients of a section 215 order can both consult with counsel and move to quash the order.

Can you please provide me with any draft language the Justice Department believes would adequately address this change in law?

ANSWER: As the Attorney General has previously stated, the Department is willing to support amendments clarifying that the recipient of a section 215 order may consult with an attorney and challenge the order in court and that the governing standard under section 215 is one of relevance. Therefore, in order to assist the Committee's consideration of these issues, we are happy to provide you with the specific language clarifying these points that the Department supports. The Department supports adoption of section 107 of

H.R. 3199, the "USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005," as passed by the U.S. House of Representatives.

(a) Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended by:

(1) striking everything after "subsection (a)(2)" in subsection (b)(2) and inserting "and that the information likely to be obtained from the tangible things is reasonably expected to be foreign intelligence information not concerning a United States person or is reasonably expected to be relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities.";

(2) amending subsection (d) to read as follows:

"(d) No person shall disclose to any person (other than those persons necessary to produce the tangible things under this section or an attorney to obtain legal advice in response to an order under this section) that the United States has sought or obtained tangible things under this section. The order shall notify the person to whom the order is directed of such nondisclosure requirement. Any recipient disclosing to those persons necessary to produce tangible things in response to an order or to an attorney to obtain legal advice in response to an order that the United States has sought to obtain tangible things under this section shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibition of disclosure."

Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended by adding the following new subsection:

"(f) (1) There is hereby established in the court established by section 103(a) a separate "Petition Review Panel" of such court, which shall consist of the three judges designated pursuant to section 103(a) who reside within 20 miles of the District of Columbia and, in the event that all of such three judges are unavailable, such other judges of the court as may be designated by the Presiding Judge of such court (who is designated by the Chief Justice of the United States from among the judges of the court). Any person who receives an order to produce any tangible thing under this section may challenge the legality of that order by filing a petition in such court. The Presiding Judge shall conduct an initial review of the petition. If the Presiding Judge determines that the petition is frivolous, the Presiding Judge shall immediately deny the petition and shall promptly provide for the record a written statement of the reasons for such decision. If the Presiding Judge determines that the petition is not frivolous, the Presiding Judge shall immediately assign the petition to one of the judges serving on the Petition Review Panel. The assigned judge shall promptly consider the petition pursuant

to procedures developed and issued by the court established pursuant to section 103(a). Such procedures for consideration of petitions shall be issued within 60 days after the enactment of, and shall be consistent with, this paragraph. Such procedures shall provide that review of petitions shall be conducted ex parte and in camera, and shall also include provisions for designation of an Acting Presiding Judge. The judge considering the petition may modify or set aside the order only if the judge finds that the order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the order, the judge shall immediately affirm the order and order the recipient to comply therewith. Any petition for review of any decision to affirm, modify or set aside an order by the United States or any person receiving such order shall be to the court of review established under section 103(b), which shall have jurisdiction to consider such petitions. The court of review shall immediately provide for the record a written statement of the reasons for its decision and, on petition of the United States or any person receiving such order for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

“(2) Judicial proceedings under this subsection shall be concluded as expeditiously as possible and shall be conducted ex parte and in camera. The judge considering any petition filed under this subsection shall provide for the record a written statement of the reasons for the decision. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision shall be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Director of National Intelligence.

“(3) All petitions under this subsection shall be filed under seal, and the court, upon the government’s request, shall review any government submission, which may include classified information, as well as the government’s application and related materials, ex parte and in camera.”

Follow up Questions from Senator Feingold

107. When the Justice Department responded to House Judiciary Committee questions about the Patriot Act in the spring of 2003, the Department explained that the "most common period of delay" courts would authorize is seven days, which was consistent with pre-Patriot Act case law. In the Department's April 4, 2005, letter to me about delayed notice search warrants, the Department stated that since 2003, "in the vast majority of instances," prosecutors were seeking delays of 30 to 90 days, and that in some instances they sought delays of up to six months or longer. At the hearing, you also stated that the average period of delay was between 30 and 90 days. Why, in the past two years, has the Justice Department changed its practice and started seeking much longer delays of notification of search warrants?

ANSWER: We do not believe the Justice Department has changed its practice relating to delayed notice search warrants. Due to the unique nature of each sensitive, ongoing criminal investigation, no one time period will be appropriate for every delayed notice search warrant. Each ongoing criminal investigation must be evaluated on an individual basis, and the federal judge reviewing the matter should be granted the discretion to tailor each delay on a case-by-case basis.

Although the information that we collected and referred to in the letter of April 2003 reflected that seven days was the period of delay commonly approved by judges, we believe the answer inaccurately included extensions (of which there were a disproportionately large number of 7-day extensions approved by judges) that skewed the data. We regret any confusion caused by the 2003 answer; however, our most recent survey covers a longer period of time and includes a larger (and therefore more reliable) sample, and makes clear that the most common initial delay sought and received was between 30 and 90 days. To the best of our knowledge, there has been no change in practice and judges continue to appropriately evaluate these decisions based on a very fact specific case-by-case analysis.

110. What other mechanisms do the Department and the FBI have in place to ensure that content is not gathered with pen/trap orders under the criminal provisions and under FISA?

ANSWER: By memorandum dated May 24, 2002, then-Deputy Attorney General Larry D. Thompson issued policy guidance to the Department concerning the avoidance of content collection in the use of pen registers and trap and trace devices:

- "As mandated by section 3121(c) [of Title 18, United States Code], an agency seeking to deploy a pen register or trap and trace device must ensure that it uses 'technology reasonably available to it' that restricts the information obtained "so as not to include the contents of any wire or electronic communications.'"

- “[T]hose responsible for the design, development, or acquisition of pen registers and trap and trace devices should ensure that the devices developed or acquired for use by the Department reflect reasonably available technology that restricts the information obtained ‘so as not to include the contents of any wire or electronic communications.’”
- “To the extent that, despite the use of ‘technology reasonably available to it,’ an agency’s deployment of a pen register does result in the incidental collection of some portion of ‘content,’ it is the policy of this Department that such ‘content’ may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security.”
- “Accordingly, each agency must take steps to ensure that any incidental collection of a portion of ‘content’ is not used for any affirmative investigative purpose.”

The FBI continues to work to ensure that the devices it develops, acquires, and uses in implementing authorized pen register and trap and trace collections reflect reasonably available technology to restrict the information obtained to information that is not content. The FBI has developed some collection capabilities to effectively isolate non-content pen/trap data from a target’s data communications. The FBI provides regular training to Technically Trained Agents regarding the Department’s policy and reminds individuals responsible for the implementation of pen/trap devices to take reasonable measures to reduce the incidental collection of any content. The FBI has also issued guidance to all field offices to establish and implement procedures that will ensure no affirmative investigative use is made of any content incidentally collected pursuant to a pen register or trap and trace.

With regard to roving wiretaps under FISA, the Justice Department has argued that when it doesn’t know the actual phone or computer to be tapped, or the identity of the person to be tapped, the statute still requires the FBI to provide a “description” of the target to the court. But the statute does not define what would be an adequate description.

111. As a matter of practice, what kind of description would an FBI agent provide in these circumstances?

ANSWER: Please see the response to question 79, above.

112. Has the Justice Department provided any formal guidelines or advice on the adequacy of a description when an agent is seeking a roving FISA tap and does not know the name or alias of the target?

ANSWER: In every instance when the Intelligence Community seeks authority to utilize the roving provisions of FISA, the Department of Justice provides the requesting agency with advice and guidance to ensure that the application adheres to all legal requirements, including the requirement to provide the court with the identity, if known, or a description of the target of the electronic surveillance. The Department has not promulgated written procedures regarding the use of the roving provision.

114. You stated at the hearing that Section 215 orders have been used to obtain "names and addresses for telephone numbers captured through court-authorized pen register devices." You also stated that "the department anticipates that the use of Section 215 will increase as we continue to use the provision to obtain subscriber information for telephone numbers captured through court-authorized pen register devices." In what circumstances would the FBI obtain a Section 215 order for this type of subscriber information, and in what circumstances would the FBI use a National Security Letter under 18 U.S.C. § 2709?

ANSWER: In addition to our unclassified response to this question, which was transmitted to the Committee on June 29, 2005, we provided information responsive to this question under separate, classified cover on July 21, 2005.

Follow up Questions from Senator Kyl

123. Before the passage of the USA PATRIOT Act, courts had interpreted FISA to mean that the surveillance could only be conducted under the statute only when foreign intelligence was the "primary purpose" of an investigation. Section 218 of the PATRIOT Act replaced the "primary purpose" requirement with a "significant purpose" standard. Has this provision had any appreciable effect in the war against terrorism? If so, please provide examples.

ANSWER: Section 218 of the USA PATRIOT Act ("the Act") has had a significant impact in the war on terrorism, as have all of the sections that helped bring down the "wall" and increase information sharing between intelligence and law enforcement. As I am sure you are aware, the Department has aggressively implemented sections 218 and 504. Following the 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. Attorney General Ashcroft 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 were reviewed as part of this process. These, and other efforts to increase coordination and information sharing between intelligence and law enforcement officers—made possible by the Act—have enabled the Department to open numerous criminal investigations, disrupt terrorist plots, bring criminal charges, and convict numerous individuals in terrorism cases. Some notable examples of these include:

- In the "Portland Seven case," in which members of a cell 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, law enforcement agents learned from a cell member, through an undercover informant, that before the plan to go to Afghanistan had been formulated, at least one member of the cell, Jeffery Battle, had contemplated attacking Jewish schools or synagogues and had been casing such buildings to select a target for such an attack. By the time investigators received this information from the informant, they 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.

If prosecutors did not act, lives could have been put at risk of a domestic terrorist attack. But if prosecutors had arrested Battle in order to prevent a potential attack, other suspects in the investigation would have likely fled or tried to conceal their activities. Because of sections 218 and 504 of the Patriot Act, it was clear that the FBI agents could conduct FISA surveillance to detect whether cell members 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 in October 2003.)

- The Department shared information pursuant to sections 218 and 504 before indicting Sami Al-Arian and several co-conspirators on charges related to their alleged involvement with the Palestinian Islamic Jihad (PIJ). In this case, sections 218 and 504 of the Patriot Act enabled prosecutors to consider all evidence against Al-Arian and his alleged co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case.
- Prosecutors and investigators used information shared pursuant to sections 218 and 504 of the Patriot Act in investigating the defendants in the "Virginia Jihad" case (*United States v. Royer, et al.*), in which members of the Dar al-Arqam Islamic Center trained for jihad in Northern Virginia by participating in paintball and paramilitary training. Eight of these individuals traveled to terrorist training camps run by the violent Islamic extremist group Lashkar-e-Taiba (LET) in Pakistan or Afghanistan between 1999 and 2001. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against these individuals. Six of the defendants have pleaded guilty, and three were convicted at trial in March 2004 of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. These nine defendants received sentences ranging from a prison term of four years to life imprisonment.

In a related prosecution, prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the Patriot Act in the case of *United States vs. Ali al-Timimi*. Timimi, the founder of the so-called Virginia Jihad, was charged with soliciting a number of these young men, five days after the attacks of 9/11, to go fight against the American troops soon expected to arrive in Afghanistan. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring a ten-count indictment against Timimi. In April 2005, a jury convicted him of soliciting others to wage war against the United States, counseling others to engage in a conspiracy to levy war against the United States, attempting to aid the Taliban, and all other charges.

- The information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the Patriot Act was useful in the prosecution of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed. An FBI undercover operation uncovered information that Al-Moayad had boasted that he had personally handed Usama Bin Laden \$20 million from his terrorist fund-raising network. 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 some of his money would be used to support HAMAS and al Qaeda, and "swore to Allah" that they would keep their dealings secret. In March 2005, both defendants were convicted of charges including conspiracy to provide material support to Hamas and conspiracy to provide material support to Al-Qaeda.

125. I have heard many people express opposition to the USA PATRIOT Act because of their concern about the status of detainees being held at Guantanamo Bay and enemy combatants, such as Jose Padilla, being held in the United States. Could you please clarify for me whether those being held at Guantanamo Bay or enemy combatants, such as Jose Padilla, are being detained pursuant to any authority contained in the USA PATRIOT Act? If the Act were to be repealed tomorrow, would it have any effect on the status of these detainees and enemy combatants?

ANSWER: You raise a common misperception. Enemy combatants, such as Jose Padilla or those detained at Guantanamo Bay, are not being held pursuant to any provision of the USA PATRIOT Act. Therefore, if the USA PATRIOT Act were to be repealed tomorrow, the authority to detain these individuals would not be altered.

127. As you know, a National Security Letter ("NSL") is basically an FBI request for information in national security investigations. Several newspapers and critics of the USA PATRIOT Act suggested last fall that a federal court in New York had held section 505 of the Act, which amended existing NSL authorities, unconstitutional on First and Fourth Amendment grounds. However, isn't it the case that it was not section 505, but rather 18 U.S.C. § 2709, the pre-existing NSL authority established by the Electronic Communications Privacy Act of 1986, which the court invalidated? Moreover, isn't it true that the Department urged an interpretation of section 2709 which would have expanded NSL recipients' rights in order to save the statute's constitutionality, and has appealed the judge's decision?

ANSWER: 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, you are correct that the amendment was not central to the court's decision striking down the law. The nondisclosure requirement invalidated by the court, for example, has existed since 1986. Notably, Jameel Jaffer, an attorney for the ACLU, has stated in connection with this case: "[T]he provisions that we challenged and that the court objected to were in the statute before the USA 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, September 30, 2004.

You are also correct that the Department of Justice interpreted the statute in question so as to protect recipients' rights. The Department of Justice took the position in the case you mention that an entity or person served with an NSL can challenge the request either: (1) as a defense to any enforcement proceeding commenced by the United States in the face of non-compliance; or (2) through a pre-production action to enjoin enforcement. The Department also took the position that the recipient of an NSL may consult an attorney regarding the request for records. The Department disagrees with the district court's interpretation of the statute as well as its constitutional holdings and has filed an appeal with the United States Court of the Appeals for the Second Circuit.

Follow up Questions from Senator Leahy

129. Section 203(b) of the PATRIOT Act authorized the disclosure of title III wiretaps to the CIA and other intelligence agencies. But unlike section 203(a), section 203(b) does not require post-disclosure notification to a court. Would you support conforming section 203(b) to section 203(a) by requiring that the court be notified when wiretap information is shared with the intelligence community? If not, why not?

ANSWER: It is now widely accepted that a lack of information sharing and coordination within our government prior to the attacks of September 11, 2001, compromised this Nation's ability to "connect the dots" and prevent terrorist attacks. See, e.g., The Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001; The National Commission on Terrorist Attacks Upon the United States (9-11 Commission) Report (collectively the "September 11 Reports"). This failure was attributable in part to legal restrictions on the disclosure of information.

Section 203(b) of the USA PATRIOT Act, codified at 18 U.S.C. § 2517(6), was one of several provisions in the Act that facilitated information sharing and helped to close the dangerous gap between law enforcement officials and members of the intelligence and national security communities. This section allowed law enforcement to disclose the contents of any court-ordered Title III wiretap, or evidence derived therefrom, to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence information to assist the official in the performance of his official duties. Disclosures under section 203(b) have been used, among other things, to track terrorists' funding sources and to identify terrorist operatives overseas.

Section 203(b) did not eliminate any of the important safeguards that exist with respect to a wiretap order, and additional safeguards must be in place before any disclosure under section 203(b) may be made. In order to obtain a wiretap, law enforcement must: (1) apply for and receive a court order; (2) establish probable cause that a particular offense has been or is about to be committed; (3) establish probable cause that communications concerning that offense will be obtained through the wiretap; and (4) provide an explanation to the court as to attempts to use other investigative procedures. Not only are wiretaps subject to prior court approval, but Title III provides for ongoing court supervision and reporting provisions.

The information sharing permitted under section 203(b) is limited. First, section 203(b) only allows for the sharing of a certain limited class of information gathered under Title III, such as information related to serious national security matters. It does not provide authority to share all information gathered under Title III authority. In addition, an individual who receives any information from a criminal investigative wiretap may

use it "only as necessary in the conduct of that person's official duties [and] subject to any limitations on the unauthorized disclosure of such information." 18 U.S.C. § 2517(6). Moreover, the Attorney General has issued binding privacy guidelines governing the sharing of information that identifies a United States person. These guidelines require that all of such information be labeled before disclosure and handled according to specific protocols designed to ensure its appropriate and limited use.

The Department believes that section 105 of the House version of H.R. 3199 would severely hamper information sharing by requiring the Federal government to file a notice with the judge who originally authorized the Title III wiretap each time a disclosure of the contents of an intercepted communication was made pursuant to section 203(b). Under section 105, the required notice would both state that contents were disclosed and indicate the departments, agencies, or entities to which the disclosure was made. We are concerned that the requirements of section 105 would prevent information from being shared in a timely manner, if at all. The September 11 Reports found that requirements similar to this notice requirement result in a culture of risk aversion; in other words, when faced with the notice requirement found in section 105, government officials might revert to an unduly conservative approach to the sharing of vital information with other law enforcement agencies, out of fear of violating the notice law and subjecting themselves to all the civil and administrative sanctions that result from Title III violations and potentially subjecting vital evidence to suppression. At the very least, delays would occur while officials sought guidance on the notice requirement's applicability and determined whether information at issue contained contents of an intercepted communication. A culture could very well develop in which information that could be shared in compliance with the provisions of the statute would nonetheless not be shared because of bureaucratic barriers. This would undermine the central purpose of the information-sharing provisions in the USA PATRIOT Act was to eliminate legal and cultural barriers to the information sharing that has become critical to our counter-terrorism efforts. Congress should not enact a notice provision that has the potential to reimpose those barriers.

The problem is compounded because section 105 contains no time limit, so even if a disclosure is made years after the conclusion of a wiretap, section 105 would still require notice to the court that authorized the wiretap. By contrast, judicial supervision of the wiretap itself is generally limited to the time period during which communications are being intercepted. One can imagine the burden that would arise in tracking disclosures and fulfilling notice requirements years after a wiretap has ended. Another concern is that this notice requirement could put sensitive information at risk. Although notice is given to the court under seal, which offers some protection, there is no prohibition or limitation on sharing the contents of the notice filing, thus possibly providing a roadmap to the Government's information-sharing efforts, on a disclosure-by-disclosure basis. These notices would not only indicate that investigators thought that communications included foreign intelligence information, but detailing the precise agencies to which the information was disclosed could also provide insight into our national security efforts. For these reasons, the Department is deeply concerned about the effects of section 105, and we cannot support it.

130. Section 203(d) of the PATRIOT Act authorized the disclosure of any foreign intelligence information obtained as part of a criminal investigation to the CIA and other intelligence agencies. You testified that section 203(d) covers information developed through law enforcement methods other than grand jury proceedings and criminal wiretaps. What kind of information is shared under section 203(d)? Absent section 203(d), what legal impediment(s) would exist to sharing such information?

ANSWER: Section 203(d) authorizes the sharing of information that was obtained during a criminal investigation with other appropriate federal officials, if the information has foreign intelligence value. Such information can be acquired in a myriad of ways, including investigative interviews, search warrants, informants, tips from the public, open source information published in the media or on the Internet, and reports from foreign police agencies.

Section 203(d) has been utilized to help investigators "connect the dots" and break up terror cells within the United States, such as those in Portland, Oregon, and Lackawanna, New York. It has also been used to revoke suspected terrorists' visas and prevent their reentry into the country. And 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 mission. Indeed, the National Counterterrorism Center may constitute the best example of section 203 information sharing, as the Center uses information provided by law enforcement agencies to produce comprehensive terrorism analysis; add to the list of suspected terrorists on the TIPOFF watchlist; and to distribute terrorism-related information across the federal government.

The question of what legal impediments to information sharing would exist if section 203(d) were allowed to sunset is difficult to answer— which merely demonstrates how important this section actually is. At a minimum, if section 203(d) is permitted to sunset, it will create confusion and uncertainty which will chill essential information sharing between the law enforcement and intelligence communities. When it comes to time-sensitive foreign intelligence information where the security of our nation is involved, we do not want our trusted officials to have to hesitate because the path is unclear. Section 203(d) is quite valuable even if it merely clarifies existing law so as to avoid any uncertainty or confusion, and therefore, it deserves renewal. Indeed, if Congress does not renew the section, its very expiration might be construed as congressional disapproval of the information sharing authorized therein — information sharing that is crucial to the ongoing war on terrorism.

Section 203(d) also protects privacy. Although historically grand jury and Title III information have been treated as more sensitive than other types of law enforcement information, section 203(d) disclosure is circumscribed in much the same way as disclosure of grand jury and Title III information under sections 203(a) and 203(b). In particular, disclosure is only authorized 1) if the information consists of foreign

intelligence, counterintelligence, or foreign intelligence information; 2) if the recipient is another federal law enforcement, intelligence, protective, immigration, national defense, or national security official; and 3) if the disclosure is meant to assist the recipient in the performance of his or her official duties. Moreover, as with grand jury and Title III information, the recipient may only use the information as necessary in the conduct of those official duties.

As the Silberman-Robb Commission pointed out, "the law already provides the framework for appropriate protection of civil liberties in the context of information sharing . . ." I believe Section 203(d) strikes the appropriate balance between the need for information sharing and protection of civil liberties.

131. Section 905 of the PATRIOT Act went even farther than section 203, by *requiring* the disclosure of foreign intelligence information obtained in a criminal investigation to the Director of Central Intelligence (subsequent legislation substituted the new Director of National Intelligence for the DCI), except as otherwise provided by law, and subject to such exceptions as the Attorney General might provide for in regulations. Does the existence of this overlapping authority create any complications for the Department? Would consolidating and conforming the authorities in sections 203 and 905 (and any accompanying regulations) add clarity to the information-sharing process?

ANSWER: Although we would be happy to discuss the issue further with the Committee, we are satisfied with the current set of authorities. As you note, section 905 of the PATRIOT Act generally requires that federal law enforcement agencies share foreign intelligence acquired in the course of a criminal investigation with the intelligence community, "[e]xcept as otherwise provided by law . . ." And as the Attorney General pointed out in Guidelines implementing section 905, section 203(d) makes it clear that no other federal or state law operates to prevent the sharing of such information, so long as the disclosure will assist the recipients in the performance of their official duties. Thus, under current law, the duty to share information under section 905 is clear. Furthermore, section 905 also has provisions that protect law enforcement equities. In short, regardless of whether the statutes could perhaps have been drafted more tightly or organized differently back in 2001, at this point we see little benefit to any changes.

132. Sections 203 and 905 of the PATRIOT Act define the kinds of information that may or must be shared with the intelligence community quite broadly. The definition of "foreign intelligence" is not limited to information about foreign governments or foreign organizations or individuals, but also includes, for example, information about Americans' contacts with overseas humanitarian organizations, information about Americans providing assistance or advice to election candidates in Iraq, and even information about Americans meeting with foreign speakers invited to American universities. When any such information ends up in the files of a law enforcement agency, these provisions of the PATRIOT Act require that it be

turned over to the CIA and other intelligence agencies. Does the FBI attempt to analyze such information, to determine its relevance to counterterrorism, before it is transferred en masse to databases in intelligence agencies throughout the government? Should it?

ANSWER: The FBI does analyze foreign intelligence that it collects pursuant to its intelligence production responsibilities. The analytic process is guided by national intelligence priorities found in the National Intelligence Priorities Framework. Foreign intelligence collected by the FBI is disseminated to other U.S. Intelligence Community (USIC) and law enforcement consumers through the FBI's standard intelligence dissemination processes. The review and approval process for intelligence dissemination includes an evaluation of the inclusion of United States Person (USP) information to comply with all applicable legal guidelines for the use of such information within the USIC.

FBI policy provides that foreign intelligence that identifies a USP shall not be disseminated to other customers of intelligence products unless a supervisory official determines, initially or upon request by a potential recipient, that such identity is or may be necessary to use, understand, or assess the importance of the intelligence.

Under some circumstances, foreign intelligence that specifically relates to terrorism is subject to special dissemination procedures, such as foreign intelligence collected through FISA. DOJ policies and procedures define the circumstances in which the FBI must provide raw terrorism material to certain agencies in the USIC. Each agency that receives such raw material has procedures in place to minimize USP information in order to avoid the improper use of this information.

Section 203 provides for: 1) the sharing of foreign intelligence or counterintelligence information 2) with certain officials in positions related to national or homeland security 3) in order to assist them in the performance of official duties. Similarly, section 905 provides for the sharing of foreign intelligence with the Director of Central Intelligence. Interactions between USPs and foreign governments, organizations, or persons cannot be arbitrarily excluded from the definitions of "foreign intelligence" and "counterintelligence" in section 3 of the National Security Act of 1947 (50 U.S.C. section 401a). The relevant data must be analyzed; it is for this reason the FBI established the Directorate of Intelligence and significantly enhanced its analytical capabilities. Obviously, every interaction between USPs and foreign entities does not involve foreign intelligence or counterintelligence and, if analysis determines that collected information does not rise to that level, it is not disseminated.

133. You testified at the hearing, "the Department estimates that Section 207 [of the PATRIOT Act] has saved nearly 60,000 attorney hours." Four days before you testified, I was informed by Director Mueller that neither the FBI nor the Department had conducted any systematic review to determine whether, and if so, how many, personnel resources had been saved by Section 207. (See Director Mueller's response to Question #86a, submitted following his testimony on May 20, 2004, and received by the Committee on April 1, 2005). Please describe the methodology by which the Department arrived at the estimate you provided at the hearing.

ANSWER: In order to arrive at the number referenced in the Attorney General's testimony, for the time period from October 26, 2001 (the effective date of the USA PATRIOT Act), to March 30, 2005, the Department of Justice first determined the number of applications filed during that time period with respect to which some of the amendments in section 207 applied. The Department then estimated the number of applications that it would have been required to file to provide the same foreign intelligence collection capability had section 207 not been implemented. The Department then multiplied the difference between those two numbers by the estimated number of hours that Department attorneys spend on preparing such applications. The Department did not attempt to estimate the number of hours spent by FBI personnel on such matters.

The Department has proposed further extending the maximum duration of FISA surveillances, stating that had these proposals been included in the PATRIOT Act, "the Department would have saved 25,000 attorney hours."

134. Please describe the methodology by which the Department arrived at this estimate.

ANSWER: Essentially the same methodology used to calculate the number of attorney hours discussed in question 133 above was used to estimate the number referenced in this question. The Department of Justice first determined the number of applications filed during that time period with respect to which the proposals, had they been included in the USA PATRIOT Act, would have applied. The Department then estimated the number of applications that it would have been required to file to provide the same foreign intelligence collection capability had the proposals been included in the PATRIOT Act. The Department then multiplied the difference between those two numbers by the estimated number of hours that Department attorneys spend on preparing such applications. The Department did not attempt to estimate the number of hours spent by FBI personnel on such matters.

135. Besides government efficiency, what considerations should guide Congress in setting the maximum duration of FISA surveillance orders and renewal orders? Do those considerations support the Department's proposal?

ANSWER: At all times, we must ensure that FISA comports with the Constitution and meets critical foreign intelligence needs. We believe that the time frames currently established by Congress for authorized periods of collection are within the framework of the Constitution, and that the amendments proposed by the Administration with respect to collection targeted at non-United States persons also comply with the Constitution. Shorter time periods or more involved reporting requirements could risk compromising legitimate intelligence collection needs and divert resources from OIPR's and FBI's other responsibilities, while substantially longer time periods might raise civil liberties concerns.

136. Section 212 of the PATRIOT Act amended 18 U.S.C. §2702 to allow an internet service provider (ISP) to voluntarily disclose the content of customer communications and associated subscriber information to the government, if the ISP reasonably believes that a life-threatening emergency justifies such disclosure. But examples of how this authority has been used suggest that it is the government, not the service provider, that generally initiates these "voluntary" disclosures. If an FBI agent tells an ISP that the immediate disclosure of customer communications and subscriber information is necessary to thwart a terrorist attack, doesn't the ISP then have the good faith, reasonable belief needed to disclose the information "voluntarily," regardless of whether the FBI agent was himself acting properly? How can section 212 be modified to prevent routine circumvention of ECPA's privacy protections?

ANSWER: The voluntary disclosure provision of Section 2702 provides the government with immediate access to e-mail content and records under emergency conditions. It explicitly permits, but does not require, a service provider to voluntarily disclose to the government information, including e-mail content, in emergencies involving an immediate risk of death or serious physical injury. These disclosures are outside of the compulsory process (i.e., subpoenas, court orders, and search warrants) that is generally required before the government can obtain such information from a service provider.

The statute permits the government to provide the service provider with the necessary information so that the service provider can determine whether there is an immediate risk of death or serious physical injury. This does not entail any circumvention of ECPA's privacy provisions, because the determination whether to disclose in light of the information provided by the government remains a voluntary decision of the service provider.

As stated in response to Question 121, above, the provision has been used to save lives.

137. Section 212 of the PATRIOT Act was amended by section 225(d) of the Homeland Security Act of 2002, Public Law 107-296 ("HSA"). The latter provision requires the Attorney General to submit a report to Congress detailing every disclosure of communications made under 18 U.S.C. §2702(b) during the one-year period after enactment of the HSA. Please provide a copy of that report.

ANSWER: This classified report was transmitted to the Congress on July 11, 2005.

138. If Congress renews section 212, would the Department object to a continuing reporting requirement with regard to communications disclosed under 18 U.S.C. § 2702(b)(8), and subscriber information disclosed under 18 U.S.C. § 2702(c)(4)?

ANSWER: Before the USA PATRIOT Act, computer-service providers could not disclose customer communications and records in emergency situations without fear of liability. If an Internet service provider (ISP) learned, for example, that a customer was about to commit a terrorist attack and notified law enforcement, the ISP might be subject to civil lawsuits - even if the disclosure saved lives.

Section 212 of the USA PATRIOT Act allows computer-service providers to disclose voluntarily both the content of a communication and customer records in life-threatening emergencies without fear of civil liability. Providers are permitted - but not required - to divulge information to a governmental entity if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. Codified at 18 U.S.C. 2702(b)(8) and 2702(c)(4), section 212 imposes no obligation on providers to review customer communications in search of such imminent dangers. Nor are ISPs compelled, in the event that the government approaches them with respect to this authority, to provide anything to the government.

Communications providers have used this authority to disclose vital information in a number of important investigations. Section 212 disclosures assisted law enforcement in locating an 88-year-old woman who had been kidnapped and was being held in an unheated shack in Wisconsin in the winter, in recovering a 13-year-old girl who had been lured and held captive by a man she met online, and in multiple investigations of credible threats of attacks directed against mosques. Section 212 disclosures have also played a vital role in securing the well-being of our youth by allowing ISPs to inform law enforcement of suicide threats.

There have been no reported or verified abuses of this provision. We therefore view as unnecessary a reporting requirement concerning either the disclosure of contents or of subscriber records pursuant to this voluntary and important provision.

139. You testified at the hearing that you could not support elevating the relevance standard under Section 215 of the PATRIOT Act to probable cause, as this "would render Section 215 a dead letter." As you know, prior to passage of the PATRIOT Act, the standard for court-ordered access to business records under section 502 of FISA was "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power." Did the FISA court issue any pre-PATRIOT Act orders under section 502? How many? Can you give us any specific examples of situations in which the pre-PATRIOT Act standard prevented the government from obtaining an order for the production of records?

ANSWER: The answer to this question is classified and was provided to the Committee under separate, classified cover on July 21, 2005.

140. The Justice Department has now twice declassified information regarding the number of FISA-court orders issued under Section 215 of the PATRIOT Act. Comparable data regarding FISA wiretaps is routinely made public in reports filed under section 107 of FISA (50 U.S.C. § 1807). Please state any objection you have to amending section 502(b) of FISA (50 U.S.C. §1862(b)) to specify that the semiannual report to the Judiciary Committee, which sets forth aggregate numbers concerning FISA orders for the production of records, shall be filed in a non-classified form.

ANSWER: We do not believe that semi-annual public reporting of the number of FISA Court orders issued under section 215 is consistent with national security interests. However, we would note that the Attorney General declassified the number of times the FBI had obtained section 215 orders as of March 30, 2005. As of that date there have been 35 such orders.

The Department of Justice, in consultation with the Intelligence Community, analyzes FISA-related statistics that can be released to the public without harming national security. At this time, it is the Department's judgment that release of any further FISA-related statistical information could pose an unacceptable risk to national security. However, the Department does make extensive reports to Congress in the Semi-Annual Report (SAR) to Congress on the use of FISA. It is our understanding that these reports are available for review by any Member and by appropriately cleared staff with a need to know through the Intelligence Committees.

Under section 305(b) of FISA (50 U.S.C. 1825(b)), if the Attorney General determines, at any time after a physical search involving the residence of a U.S. person is conducted under FISA, that there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to such person of the fact of the search and identify any property seized, altered, or reproduced during such search.

142. How many times since September 11, 2001, has the Attorney General provided notice to a U.S. person pursuant to this provision?

ANSWER: The Attorney General has relied on 50 U.S.C. § 1825(b) three times since September 11, 2001, to provide notice of the search of the residence of a United States person.

144. What criteria does the Attorney General use in making a determination under this provision, and is there a regular process for making such a determinations?

ANSWER: The answer to this question is classified and will be provided under separate, classified cover.

145. Section 505 of the PATRIOT Act broadly expanded the FBI's authority to issue administrative subpoenas (known as "national security letters," or "NSLs") in terrorism investigations. The FBI has read section 505 to authorize the service of NSLs on libraries that offer their patrons access to the Internet. Has the FBI used NSLs to obtain library records, how often, and under what circumstances?

ANSWER: The answer to this question is classified and was provided to the Committee under separate, classified cover on July 21, 2005.

146. Librarians have argued that libraries are not ISPs, that libraries offering Internet access are themselves customers of ISPs, and that the FBI can obtain the information it needs from the ISPs that service the libraries. What information can the FBI *not* obtain through an NSL served on an ISP that services a library that it *can* obtain through an NSL served on the library itself?

ANSWER: The answer to this question depends upon the extent to which the library acts as its own internet service provider (ISP) and the nature of the connection, if any, between the library and another ISP that furnishes services to the library. When the library acts as its own ISP, it will have all of the pertinent records. When another ISP provides services to the library, in some instances the ISP will have most of the pertinent records and in others, the library may have significant records regarding usages that the ISP will not have or retain.

152. The Department has argued that Federal Rule of Criminal Procedure 6(e) prohibits it from revealing the exact numbers of material witnesses who are detained pending their testimony before a grand jury. The Supreme Court has identified five reasons for grand jury secrecy: "(1) To prevent the escape of those whose indictment may be contemplated; (2) to insure the utmost freedom to the grand jury in its deliberations, and to prevent persons subject to indictment or their friends from importuning the grand jurors; (3) to prevent subornation of perjury or tampering with the witnesses who may testify before [the] grand jury and later appear at the trial of those indicted by it; (4) to encourage free and untrammelled disclosures by persons who have information with respect to the commission of crimes; [and] (5) to protect innocent accused who is exonerated from disclosure of the fact that he has been under investigation, and from the expense of standing trial where there was no probability of guilt." *Douglas Oil Co. v. Petrol Stops Northwest*, 441 U.S. 211, 219 n.10 (1979) (internal quotations omitted). Please explain how withholding generalized information regarding the use of the material witness statute, e.g., the numbers of material witnesses arrested and detained, furthers any legitimate purpose secured by the grand jury secrecy rule.

ANSWER: We appreciate the opportunity to address this issue. The Department is committed to keeping Congress informed about the issue of material witness warrants, while also respecting the letter and spirit of the grand jury secrecy rules and Fed. R. Crim. P. 6(e) and protecting our vital national security interests.

As the courts have pointed out, "the scope of [grand jury] secrecy is necessarily broad. It encompasses not only the direct revelation of grand jury transcripts but also the disclosure of information which would reveal 'the identities of witnesses or jurors, the substance of testimony, the strategy or direction of the investigation, the deliberations or questions of the jurors, and the like.'" *Fund for Constitutional Gov't v. Nat'l Archives & Records Serv.*, 656 F.2d 856, 859 (D.C. Cir. 1981) quoting *SEC v. Dresser Indus.*, 628 F.2d 1368, 1382 (D.C. Cir. 1980). The Department is, therefore, legally obligated to refrain from disclosing information that would reveal the strategy or direction of a grand jury investigation, or otherwise run afoul of the broad scope of the rule.

As your question implies, the grand jury secrecy rules serve very important governmental and societal interests. One important interest you reference is protecting the privacy of individuals who have participated in grand jury proceedings. However, it is worth noting that witnesses are not bound by Rule 6(e)—that these witnesses have not stepped forward and identified themselves indicates that their privacy has been well served by our strict adherence to Rule 6(e).

And in terrorism investigations in particular, following the rules on grand jury secrecy also serves important national security interests. Terrorists and their supporters, who would seek to harm the United States, are interested in learning every detail of our efforts to detect, disrupt, and prosecute them. Obeying the rules on grand jury secrecy keeps valuable information out of their hands. There is also information that may be at the margins of Rule 6(e) protection that nonetheless may not be disclosed because of the

harm that would inflict on our efforts to keep Americans safe. Often, in the grand jury context, these two rationales will overlap, which has been the case with respect to numerous information requests made in the past.

Because of the rules on grand jury secrecy, we cannot release the number of material witnesses who have been detained pending testimony before a grand jury in any particular case, such as the investigation into the September 11th attacks. Revealing the total number of grand jury material witness warrants issued in a particular investigation and where those warrants are being issued, could potentially reveal the strategy and progress of the investigation—particularly if the number was released with regularity. It would then be possible to track the progress of an individual investigation by measuring the incremental increase or decrease in the number of warrants sought or secured. Furthermore, disclosing such information would impede the war on terror and hinder the Department's investigation of the September 11th attacks. As such, it continues to be our legal obligation to protect the specific number of material witnesses detained as part of the 9/11 investigation, the districts to which they relate, and the length of those witnesses' detention.

However, to the extent Congress is seeking aggregate numbers of material witness warrants across terrorism cases, the Department believes that it can disclose some of this information consistent with grand jury secrecy rules and with national security. Specifically, we have concluded that at this point in time, several years after the 9/11 attacks and in the wake of numerous grand jury investigations in terrorism cases that would blur attempts to reverse engineer our investigative efforts, a release of the aggregate number of material witnesses detained in all post-9/11 terrorism investigations would not disclose a matter before the grand jury, and thus would not violate Federal Rule of Criminal Procedure 6(e).

Of course, the numbers that follow are only approximate because the Department does not collect comprehensive data on the frequency with which U.S. Attorneys' Offices utilize the longstanding material witness authority under 18 U.S.C. § 3144. Nevertheless, in an effort to obtain information on the extent of use of this tool, we recently surveyed U.S. Attorneys' Offices and according to our informal survey, only in approximately 90 instances have material witness warrants been used in terrorism-related investigations since 9/11/2001. Twenty-eight districts reported that they have not used the material witness statute to detain anyone since 9/11/2001. In addition, our survey indicated that material witness warrants have been used approximately 230 times in investigations involving crimes such as drugs, guns, and violent crimes since 9/11/2001. As the Committee has known for years, material witness warrants continue to be used regularly in alien smuggling cases. Indeed, our survey indicated that approximately 9,600 of the approximately 10,000 material witness warrants that have been issued since 9/11/2001 have been in alien smuggling and immigration related investigations.

The frequency with which these material witnesses have testified before the Grand Jury is difficult to estimate. As with the use of material witness warrant authority, the Department does not collect comprehensive data on this, and we cannot even venture

approximate figures. There are many reasons why an individual detained as a material witness might not testify before a grand jury. It might well be the case that a material witness might not have testified before the grand jury because he or she struck a deal with the prosecution to become an informant, or because the thrust of his or her testimony may have been conveyed by another grand jury witness. In alien smuggling cases, which represent the vast majority of investigations in which material witness warrants are used, the individuals generally are detained for deposition and then released and deported. Given that the enabling statute requires very close supervision by the courts of the issuance of material witness warrants and affords significant procedural protections to material witnesses, we are confident that this authority is being properly used. From the outset, a court must issue a material witness arrest warrant – this is not a tool that a prosecutor can simply use absent prior court authorization. By statute, a material witness is entitled to an attorney; in the event that he or she cannot afford an attorney, one will be provided. By statute, the individual is also entitled to a hearing before a judge. And the Federal Rules of Criminal Procedure require prosecutors to file frequent reports to the judge, keeping that judge apprised of the status of those detained as material witnesses.

153. Please state and explain any objection you might have to the following reporting language: "Notwithstanding any other provision of law, the Attorney General shall report annually to the Committees on the Judiciary of the House of Representatives and the Senate concerning the use of the material witness statute, 18 U.S.C. § 3144. Such report shall include, with respect to the preceding 1-year period: (1) the total number of affidavits in support of a material witness warrant filed by an attorney for the government; (2) the total number of material witness warrants either granted or denied; (3) the total number of persons arrested as material witnesses and detained in accordance with the provisions of 18 U.S.C. § 3142, whose testimony was secured, either by deposition or by appearance before the grand jury; and (4) the total number of persons arrested as material witnesses and detained in accordance with the provisions of 18 U.S.C. § 3142, whose testimony was not secured, either by deposition or by appearance before the grand jury, and the reasons therefor."

ANSWER: We are hesitant to support a reporting requirement for several reasons.

First, it is unnecessary given the very close supervision by the courts of the issuance of material witness warrants and the significant procedural protections afforded material witnesses. From the outset, a court must issue a material witness arrest warrant—this is not a tool that a prosecutor can simply use absent prior court authorization. By statute, a material witness is entitled to an attorney; in the event he or she cannot afford an attorney, one will be provided. By statute, the individual is also entitled to a hearing before a judge. The Federal Rules of Criminal Procedure require prosecutors to file frequent reports to the judge, keeping that judge apprised of the progress of the grand jury proceedings. There is already significant contemporaneous oversight of any use of material witness warrants.

Second, the proposed reporting requirement is deeply problematic and would require the reporting of information at the core of Rule 6(e) protections. For example, any requirement to explain why the testimony of some persons arrested on material witness warrants was not secured would implicate grand jury information and could harm national security. It may well be the case that a material witness might not have testified before the grand jury because he or she struck a deal with the prosecution to become an informant, or because the thrust of his or her testimony may have been conveyed by another grand jury witness. These kinds of situations go to the heart of Rule 6(e) and the need for grand jury secrecy.

Finally, the Department is very concerned about the ever increasing number of reporting requirements the Congress continues to impose. While we are respectful of Congress' oversight role, the burden placed on the Department by numerous disjointed reporting requirements is significant. Because reporting requirements necessarily reduce the time available to prosecutors and investigators to pursue cases, the Department does not support imposition of a new reporting requirement with respect to this provision.

On March 5, 2005, the *New York Times* reported that the Bush Administration's secret program to transfer suspected terrorists to foreign countries for interrogation has been carried out by the CIA under broad authority that has allowed it to act without case-by-case approval from the White House or the State or Justice Departments. The article states that the CIA's authority to operate independently was provided by the White House under a still-classified directive signed by President Bush within days of the September 11 attacks.

154. As White House Counsel, were you aware of this authority granted to the CIA?

ANSWER: Activities of the CIA are subject to the oversight of the intelligence committees. It would be most appropriate to address classified matters regarding the CIA through that oversight process.

155. As Attorney General, do you believe the CIA should be allowed to secretly transfer detainees without first obtaining approval by the State or Justice Departments?

ANSWER: Activities of the CIA are subject to the oversight of the intelligence committees. It would be most appropriate to address classified matters regarding the CIA through that oversight process.

156. President Bush indicated at his press conference on March 17, 2005, that the United States only transfers detainees back to their own countries. Is this true, or does our government also transfer detainees to other countries of which they are not nationals? What objective would we have for sending a detainee to a country of which he is not a national?

ANSWER: We do not believe that at his press conference on March 16, 2005, the President stated that the United States *only* transfers individuals back to their own countries. Rather, he merely referred to transferring persons "back to their country of origin" as an example of an action the U.S. might take when he was responding to a general question about the practice of "rendition."

Transferring an individual to the custody of a nation other than his country of nationality may be appropriate in some circumstances. For example, circumstances may arise in which the United States comes into custody of an individual overseas who is wanted for prosecution in a third country. If the United States does not have an extradition treaty with that country, or if the terms of any extradition treaty are inapplicable given the extraterritorial nature of the custody, transfer to that country for prosecution may nevertheless be in the interests of the United States and legally appropriate. Of course, as the Administration has made clear, it is the policy of the United States not to transfer an individual to a country if the United States determines that it is more likely than not that the individual will be tortured.

157. In my written follow-up questions after your confirmation hearing, I asked if you supported the creation of an independent commission to investigate U.S. detention and interrogation practices at U.S.-operated detention facilities. You replied that you "do not currently have reason to believe that the proposed commission is advisable, but [you] reserve judgment on that question." Since answering that question, the government has released hundreds of documents in response to a FOIA lawsuit that show widespread abuse in Iraq, Afghanistan, and Guantanamo Bay. In March, the ACLU released a September 14, 2003, memo from General Sanchez that contradicts his testimony before the Senate Armed Services Committee on May 19, 2004. We also learned recently that Army commanders have decided not to prosecute 17 American soldiers implicated in the deaths of three prisoners in Iraq and Afghanistan in 2003 and 2004. In these cases, investigators had recommended that all 17 soldiers be charged, including charges as serious as murder, conspiracy, and negligent homicide. These are only a few of the recent developments in the prisoner abuse scandal. You reserved judgment on my question about an independent commission in January. Do you now support the creation of an independent commission to investigate U.S. detention and interrogation practices at U.S.-operated detention facilities?

ANSWER: The President has recently and repeatedly reaffirmed the longstanding policy that the United States will neither commit nor condone torture. We do not tolerate torture. The Administration and the Department of Justice are committed to investigating

and punishing torture or improper treatment of detainees. We have been doing so vigorously. The United States has conducted a number of investigations focusing on allegations of torture or abuse. These investigations have assisted in identifying credible allegations of abuse. Individuals found to have acted unlawfully were or are being held accountable. Depending on the severity of the offense, penalties have ranged from criminal to administrative sanctions. An independent commission is therefore not necessary.

In addition, as expressed in the Statement of Administration Policy on S. 1042, the "National Defense Authorization Act for Fiscal Year 2006," the Administration opposes legislative proposals to establish a national commission to investigate detainee operations or to regulate the detention, treatment, or trial of terrorists captured in the war on terror. Such legislation would interfere with the protection of Americans from terrorism by diverting resources from the war to answer unnecessary or duplicative inquiry or by restricting the President's ability to conduct the war effectively under existing law.

During your confirmation proceedings, you argued that the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment does not prohibit cruel, inhuman or degrading treatment or punishment "with respect to aliens overseas." An April 4, 2005, letter from Assistant Attorney General Moschella reiterates this flawed interpretation. The legislative history of the treaty's ratification clearly indicates that the purpose of the Senate reservation was to prevent any tribunal or country from claiming that the United States would have to follow a different and broader meaning of the language of Article 16 than the meaning of the words "cruel and unusual punishment" contained in the Constitution. The Department of Justice at the time characterized this reservation as "modest," and explained its purpose as being to use established meanings under the Eighth Amendment instead of the Convention Against Torture's vague terms that had not yet evolved under international law. The reservation was only intended to provide a substantive definition of the term "cruel, inhuman or degrading treatment or punishment" in Article 16, not to impose a geographical limitation on the obligations of the United States under Article 16.

158. Will you direct the Office of Legal Counsel to reconsider its interpretation of the Senate reservation to Article 16 of the Convention to ensure that it reflects the original intent of the Senate?

ANSWER: Article 16 of the Convention Against Torture requires each Party to the Convention to "undertake to prevent in any territory under its jurisdiction other acts of cruel, inhuman or degrading treatment or punishment." As noted in the April 4, 2005, letter from Assistant Attorney General Moschella, Article 16 is limited in its reach. It imposes obligations on the United States only "in any territory under its jurisdiction." Furthermore, pursuant to the reservation required by the Senate, the United States is bound by its obligations under Article 16 "only insofar as the term 'cruel, inhuman or

degrading treatment or punishment' means the cruel, unusual and inhumane treatment or punishment prohibited by the Fifth, Eighth, and/or Fourteenth Amendments to the Constitution." This reservation was adopted because of concern over the uncertain meaning of the phrase "cruel, inhuman or degrading treatment or punishment," and was intended to ensure that existing constitutional standards would satisfy U.S. obligations under Article 16. *See, e.g.*, S. Exec. Rep. No. 101-30, at 8 (1990) ("In view of the ambiguity of the terms, the administration believes that U.S. obligations under this article should be limited to conduct prohibited by the U.S. Constitution."). As the State Department Legal Adviser testified, "[B]ecause the Constitution of the United States directly addresses this area of law, and because of the ambiguity of the phrase 'degrading,' we would limit our obligation under the Convention to the proscriptions already covered by our Constitution." *Convention Against Torture: Hearing Before the Senate Comm. on Foreign Relations*, 101st Cong. 11 (1990) (statement of Abraham D. Sofaer). Regardless of the precise scope of U.S. obligations under Article 16, however, it is the policy of the Administration to abide by the substantive constitutional standard incorporated into Article 16 even if such compliance is not legally required, regardless of whether the detainee in question is held in the United States or overseas.

159. What interest would our government have for excluding the protections of Article 16 to alien detainees held abroad?

ANSWER: The United States Government is committed to complying faithfully with its treaty obligations, including those under Article 16 of the Convention Against Torture. Furthermore, as noted above, it is the policy of the Administration to abide by the substantive constitutional standard incorporated into Article 16 even if such compliance is not legally required, regardless of whether the detainee in question is held in the United States or overseas.

162. Another question (#25) I submitted following your confirmation hearing asked, "What changes do you believe should be made to our cocaine sentencing laws, if any?" You replied, "I have not myself studied the issue carefully." Have you considered the issue since your confirmation and, if so, would you please respond now to the question?

ANSWER: Existing cocaine sentencing laws reflect the fact that crack is a more dangerous and harmful substance than powder cocaine. For law enforcement purposes, it makes little difference that crack (cocaine base) and powder (cocaine hydrochloride) are chemically similar. Crack is more addictive, causing heavier and more frequent use. Crack also results in more emergency-room episodes and treatment admissions at public facilities than powder cocaine, even though powder cocaine is much more widely used. To the extent that a change in sentencing may be necessary, it may be more appropriate to address the differential between crack and powder penalties by increasing the penalties for powder cocaine.

I was dismayed to learn that the United States has retreated further from the international community by the President's decision to withdraw from the Optional Protocol to the Vienna Convention on Consular Relations. The decision to withdraw from the Protocol was prompted by last year's ruling by the International Court of Justice (ICJ) that the U.S. had violated the Convention with regard to 51 Mexican nationals on death row who were not afforded their consular rights.

Just a few days before announcing that the U.S. was withdrawing from the Protocol, the Administration announced that it would prevail upon Texas to comply with that ICJ ruling. Both announcements came on the eve of the oral argument before the U.S. Supreme Court in a case brought by the Mexican nationals against Texas, to enforce the ICJ's ruling.

171. Were you consulted about these developments – that is, the decision to withdraw from the Protocol, and the decision to direct Texas to comply with the ICJ ruling? Did you concur in these decisions?

ANSWER: The United States remains a party to the Vienna Convention on Consular Relations (VCCR). The Optional Protocol to the VCCR gives the International Court of Justice (ICJ) jurisdiction to decide disputes concerning the "interpretation and application" of the VCCR.

Pursuant to the Optional Protocol, Mexico in 2003 initiated proceedings against the United States in the *Case Concerning Avena and Other Mexican Nationals (Mexico v. United States of America) (Avena)*, asking the ICJ to resolve a dispute concerning the interpretation and application of the VCCR as it pertained to certain Mexican nationals who had been convicted and sentenced under the laws of several States of the United States. On March 31, 2004, the ICJ issued its judgment, 2004 I.C.J. 128 (Mar. 31), finding that the United States had breached Article 36 of the VCCR and that the appropriate remedy is for the United States "to provide, by means of its own choosing, review and reconsideration of the convictions and sentences of the Mexican nationals."

The President of the United States, through subordinate Executive Branch officials, represents the United States in ICJ proceedings and in the United Nations, and he has the lead role in determining whether, and if so how, to comply with the determinations of such international bodies. The Department of Justice's Office of Legal Counsel (OLC) assists the Attorney General in his function as legal advisor to the President, and OLC typically plays a role in analyzing the obligations of the United States under international law.

The President determined that United States will discharge its international obligations under the ICJ in *Avena* "by having State courts give effect to the decision in accordance with general principles of comity in cases filed by the 51 Mexican nationals addressed in that decision." Memorandum to the Attorney General, Feb. 28, 2005. By

letter dated March 7, 2005, the Secretary of State informed the Secretary-General of the United Nations that the United States "hereby withdraws from the [Optional] Protocol. As a consequence of this withdrawal, the United States will no longer recognize the jurisdiction of the International Court of Justice reflected in that Protocol." The Administration's position on these issues was communicated by the Attorney General to those States affected by the ICJ's *Avena* judgment. The extent of the President's consultation with the Attorney General and the advice provided him before he made those decisions are confidential. To preserve the President's ability to obtain confidential legal advice from the Department, the Department does not disclose such matters.

172. Did the pendency of the Supreme Court case enter into the Administration's decisions in any way? Please explain.

ANSWER: The United States Supreme Court granted certiorari in *Medellin v. Dretke*, 371 F.3d 270 (5th Cir. 2004), to resolve issues concerning interpretation of the Antiterrorism and Effective Death Penalty Act of 1996, 28 U.S.C. 224 et seq. (AEDPA), and obligations of the United States under the Vienna Convention on Consular Relations (VCCR). The United States has a substantial interest in the interpretation and effect given to international instruments to which it is a party, and in presenting arguments on such issues to the Supreme Court. Accordingly, it was important that the United States determine its position regarding the VCCR and the implications of the ICJ's *Avena* judgment before the Supreme Court heard argument in the *Medellin* case on March 28, 2005.

175. In the classified set of answers to questions submitted to Director Mueller after his appearance before the Judiciary Committee on May 20, 2004, a document was attached as "Enclosure #5 to the 5/30/03 EC." Please review this document for declassification and release it to the public, in redacted form if necessary.

ANSWER: That particular attachment was not classified and is provided as an Enclosure. (Enclosure 4)

164

ENCLOSURE 1

EFF Section 215-774



U.S. Department of Justice
Office of Legislative Affairs

RECEIVED

2005 JUL -5 AM 11: 57

Office of the Assistant Attorney General

Washington, D.C. 20530

OIPR
DEPT OF JUSTICE

~~SECRET~~

MAY 24 2005

Senator Pat Roberts, Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Roberts:

I write to express the Department of Justice's strong opposition to any attempt to impose an "ascertainment" requirement on the implementation of multi-point or "roving" surveillance conducted under the Foreign Intelligence Surveillance Act (FISA). (U)

As the Members of this Committee are well aware, a roving surveillance order attaches to a particular target rather than to a particular phone or other communications facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Before the USA PATRIOT Act, however, FISA did not include a roving surveillance provision. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. However, international terrorists and spies are trained to thwart surveillance by regularly changing communication facilities, especially just prior to important meetings or communications. Therefore, without roving surveillance authority, investigators were often left two steps behind sophisticated terrorists and spies. (U)

Thankfully, section 206 of the USA PATRIOT Act ended this problem by providing national security investigators with the authority to obtain roving surveillance orders from the FISA Court. This provision has put investigators in a much better position to counter the actions of spies and terrorists who are trained to thwart

~~SECRET~~

Classified by: James A. Baker, Counsel for Intelligence Policy,
Office of Intelligence Policy and Review, U.S.
Department of Justice

Reason: 1A(e)

Declassify on: XI

Declassified by: James A. Baker
Counsel for Intelligence Policy
OIPR/USDOJ
Date: 7/9/05

~~SECRET~~

surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times and has proven effective in monitoring foreign powers and their agents. (U)

Some in Congress have expressed the view that an "ascertainment" requirement should be added to the provisions in FISA relating to "roving" surveillance authority. Section 2 of the S. 737, the Security and Freedom Ensured Act of 2005 ("SAFE Act"), for example, would provide that such surveillance may only be conducted when the presence of the target at a particular facility or place is "ascertained" by the person conducting the surveillance. (U)

Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" surveillance orders that pertains to "roving" wiretap orders issued in criminal investigations, but this is wholly inaccurate. The relevant provision of the criminal wiretap statute states that the roving interception of oral communications "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." See 18 U.S.C. § 2518(12). With respect to the roving interception of wire or electronic communications, however, the criminal wiretap statute imposes a more lenient standard, providing that surveillance can be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." See 18 U.S.C. § 2518(11)(b)(iv). (U)

Any "ascertainment" requirement, however, whether it is the one contained in the SAFE Act or the one currently contained in the criminal wiretap statute, should not be added to FISA. Any such requirement would deprive national security investigators of necessary flexibility in conducting sensitive surveillance. Due to the different ways in which foreign intelligence surveillance and criminal law enforcement surveillance are conducted as well as the heightened sophistication of terrorists and spies in avoiding detection, provisions from the criminal law cannot simply be imported wholesale into FISA. (U)

Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world. As a result, they generally engage in detailed and extensive counter-surveillance measures. Adding an ascertainment requirement to FISA therefore runs the risk of seriously jeopardizing the Department's ability to effectively conduct surveillance of these targets because, in attempting to comply with such a requirement, agents would run the risk of exposing themselves to sophisticated counter-surveillance efforts. (U)

~~SECRET~~

~~SECRET~~

In addition, an ascertainment requirement is unnecessary in light of the manner in which FISA surveillance is conducted. As the Members of this Committee are no doubt aware, intercepted communications under FISA are often not subject to contemporaneous monitoring but rather are later translated and culled pursuant to court-ordered minimization procedures. These procedures adequately protect the privacy concerns that we believe the proposed ascertainment provisions are intended in part to address. (U)

While we understand the concern that conversations of innocent Americans might be intercepted through roving surveillance under FISA, the Department does not believe that an ascertainment requirement is an appropriate mechanism for addressing this concern. Rather, we believe that the current safeguards contained in FISA along with those procedures required by the FISA Court amply protect the privacy of law-abiding Americans. (U)

First, under section 206, the target of roving surveillance must be identified or described in the order of the FISA Court, and if the target of the surveillance is only described, such description must be sufficiently specific to allow the FISA Court to find probable cause to believe that the specified target is a foreign power or agent of a foreign power. As a result, section 206 is always connected to a particular target of surveillance. Roving surveillance follows a specified target from phone to phone and does not "rove" from target to target. (U)

Second, surveillance under section 206 also can be ordered only after the FISA Court makes a finding that the actions of the specified target may have the effect of thwarting the surveillance (by thwarting the identification of those persons necessary to assist with the implementation of surveillance). (U)

Additionally, all "roving" surveillance orders under FISA must include Court-approved minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. These are usually in the form of standard minimization procedures applicable to certain categories of surveillance, but the procedures may be modified in particular circumstances. (U)

(b)(1)1.4c

~~SECRET~~

~~SECRET~~

(b)(1)7.4c



In sum, the Department believes that the safeguards set forth in this letter reflect the appropriate balance between ensuring the effective surveillance of sophisticated foreign powers and their agents and protecting the privacy of the American people. The Department strongly opposes any attempt to disturb this balance by adding an ascertainment requirement to the provisions of FISA relating to roving surveillance authority. (U)

We hope that this information will be useful to the Committee as it considers the reauthorization of those USA PATRIOT Act provisions scheduled to sunset at the end of this year. Please do not hesitate to contact me if you have additional questions or concerns about this issue. (U)

Sincerely,

William E. Moschella
William Moschella
Assistant Attorney General

~~SECRET~~

169

ENCLOSURE 2

EFF Section 215-779



Office of the Attorney General
Washington, D. C. 20530

July 12, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

The Department of Justice has carefully reviewed S. 737, the Security and Freedom Ensured Act of 2005 ("SAFE Act"), introduced by Senators Craig and Durbin. While this legislation does contain certain principles with which the Department agrees, the Department has concluded that the SAFE Act would roll back or weaken many of the most important and useful authorities enacted by the USA PATRIOT Act. Indeed, some provisions of the SAFE Act would make it *more* difficult to combat terrorism and violent crime than was the case before the USA PATRIOT Act was passed. In this letter, we highlight only some of the legislation's most objectionable features. Although, as I previously announced, we continue to support clarifying certain authorities contained in the USA PATRIOT Act, we urge the Senate to reject the SAFE Act and retain the vital tools needed to safeguard the American people and the values we cherish. If S. 737 is presented in its current form to the President, the President's senior advisors will recommend that it be vetoed.

Section 2. Section 206 of the USA PATRIOT Act provided national security investigators with the authority to conduct court-approved multi-point (sometimes called "roving") surveillance of foreign powers or agents of foreign powers, such as terrorists or spies, who may take steps to thwart surveillance. Multi-point wiretap authority has been available in criminal investigations since 1986, and section 206 simply added this authority to FISA. As of March 30, 2005, the Department had used section 206 of the USA PATRIOT Act 49 times, and it has been effective in investigating international terrorists and spies, who are often trained to take sophisticated measures to evade detection.

Section 2 of the SAFE Act would significantly impair the Department's ability to conduct surveillance of terrorists and spies in two ways. First, it would eliminate the use of "roving" wiretaps in cases where the Government is able to specify the target only by a description and cannot provide his true identity. Currently, when applying to the FISA Court for a surveillance order, the Government

The Honorable Arlen Specter

Page 2

must provide the court with the target's identity if known, or otherwise a description of the target. The ability to provide a description could be critical in cases where the Government knows a great deal about a target but does not know his identity because, for example, he is a spy trained to conceal it. And the possibility of providing a description does not reduce the safeguards placed on section 206's "roving" wiretap authority. Every "roving" surveillance order is tied to a particular target. The court order authorizing surveillance then allows surveillance of the target to continue if he switches phones; it does not allow the Government to switch surveillance to a different target. Moreover, to authorize surveillance ("roving" or not) the FISA Court must find probable cause that the target of the surveillance is a foreign power or an agent of a foreign power. Thus, in cases where the Department does not know the identity of the target, the Department is required to present a sufficiently particular description of a target to allow the FISA Court to make the determination that the specified target is a foreign power or an agent of a foreign power. And the FISA Court may authorize "roving" surveillance only where it finds that the target's actions, such as a pattern of frequently changing cell phones, may thwart surveillance.

Section 2 of the SAFE Act would require that an electronic surveillance order under FISA specify either: (1) the identity of the target of the surveillance; or (2) the location of each of the facilities or places at which surveillance will be directed. Thus, if investigators did not know the true identity of the target, investigators would not be able to obtain a "roving" wiretap based on a description, and the Government's ability to surveil the suspected international terrorist or spy would be diminished. Due to the nature of a roving target using various and changing facilities to carry out his terrorist or clandestine intelligence activities, it is oftentimes impossible to specify the facility or location at which surveillance will be directed at the time that the FISA order is executed. In that case, every time the target attempted to thwart surveillance by switching to a new cell phone number, the Government would be required to take the time to prepare and submit a new surveillance application to the FISA Court, with the likely effect that investigators would lose the ability to monitor key conversations.

This provision of the SAFE Act would also diminish the effectiveness of "roving" surveillance by providing that such surveillance could only be conducted when the presence of the target at a particular facility or place is "ascertained" by the person conducting the surveillance. Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" surveillance orders that pertains to "roving" wiretap orders issued in criminal investigations, but this is inaccurate. The relevant provision of the criminal wiretap statute states that the interception of an *oral* communication (such as by bugging) "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." See 18 U.S.C. § 2518(12). With respect to the roving interception of *wire or electronic* communications, the criminal wiretap statute imposes a more lenient standard, providing that surveillance can be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." See 18 U.S.C. § 2518(11)(b)(iv).

The Honorable Arlen Specter
Page 3

The proposed ascertainment requirement, as well as provisions from the criminal wiretap statute referenced above, would deprive investigators of necessary flexibility in conducting sensitive surveillance. Due to the different ways in which foreign intelligence surveillance and criminal law enforcement surveillance are conducted as well as the heightened sophistication of terrorists and spies in avoiding detection, provisions from the criminal law cannot simply be imported wholesale into FISA. Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world. Consistent with this fact, they generally engage in detailed and extensive counter-surveillance measures. Adding an ascertainment requirement to FISA therefore runs the risk of seriously jeopardizing the Department's ability to effectively conduct surveillance of these targets because, in attempting to comply with such a requirement, agents could run the risk of exposing themselves to sophisticated counter-surveillance efforts.

FISA already protects the privacy of innocent Americans in numerous ways. First, the target of roving surveillance must be identified or described in the order of the FISA Court. Second, the FISA Court must find that there is probable cause to believe the particular target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Third, roving surveillance can be ordered only after the FISA Court makes a finding that the actions of the target of the application may have the effect of thwarting surveillance. Additionally, all "roving" surveillance orders under FISA must include court-approved minimization procedures that limit the acquisition, retention, and dissemination by the Government of information or communications involving United States persons.

Congress should not impose restrictions that make it more difficult for investigators to conduct "roving" wiretaps directed against international terrorists than it is to conduct such wiretaps against drug dealers and those participating in organized crime. Neither should Congress adopt provisions from other areas of the law that would jeopardize surveillance conducted against our Nation's most dangerous and well-trained enemies. The Department would oppose any changes in the law that would make it more difficult for the Government to conduct effective surveillance of international terrorists. As a result, the Department is unable to support section 2 of the SAFE Act.

Section 3. Section 3 would require investigators in certain circumstances to tip off criminals by immediately notifying them of a search even if such notice would "seriously jeopardize an investigation." Delayed-notice search warrants -- by which courts allow investigators temporarily to delay providing notice that a search has been conducted if immediate notice would have an "adverse result" -- had been available for decades before the USA PATRIOT Act was passed. Section 213 of the USA PATRIOT Act merely created a nationally uniform process and standard for obtaining them. The SAFE Act would narrow the types of "adverse results" justifying a delayed-notice warrant. Currently, a delayed-notice warrant can be issued only where immediate notification may result in: "endangering the life or physical safety of an individual"; "flight from prosecution"; "destruction of or tampering with evidence"; "intimidation of potential witnesses"; or "otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(a)(2). The SAFE Act would allow delayed notice only

The Honorable Arlen Specter

Page 4

under the first four circumstances. Thus, even if a court found that immediate notification would "seriously jeopardiz[e]" an investigation, the law would prohibit the court from authorizing even a temporary delay. Investigators would therefore be put in the position of deciding whether to forego the search altogether or to conduct the search and provide immediate notice, potentially tipping off suspects and thus enabling them and their associates to go into hiding, flee, change their plans, or even accelerate their plots. Again, this limitation would make the law more restrictive than it was before the USA PATRIOT Act.

Although it is simply not possible to predict every way in which immediate notice could seriously jeopardize an investigation, experience has shown that there are certain adverse effects of notice that would seriously jeopardize an investigation but would not otherwise constitute a ground for delaying notice if the SAFE Act were enacted. One such situation arose in the Western District of Pennsylvania. 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 revealed and endangered a related Title III wiretap that was ongoing for major drug trafficking activities.

An Organized Crime Drug Enforcement Task Force was engaged in a multi-year investigation that culminated in the indictment of the largest drug trafficking organization ever prosecuted in the Western District of Pennsylvania. While the drug investigation was ongoing, it became clear that several leaders of the drug 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 the search into the credit card fraud investigation revealed the ongoing drug investigation prematurely, the drug investigation could have been seriously jeopardized. As a result of the drug trafficking investigation, a total of 51 defendants were indicted on drug, money laundering and firearms charges. The organization's heads were charged with operating a Continuing Criminal Enterprise as the leaders of the organization; both pleaded guilty and received very lengthy sentences of imprisonment. The case had a discernable and positive impact upon the North Side of Pittsburgh, where the organization was based. For example, heroin overdose deaths in Allegheny County declined from 138 in 2001 to 46 in 2003. The credit card investigation, in turn, ultimately resulted in several cases, and all but one of the defendants charged with credit card fraud were convicted.

The SAFE Act would have prevented law enforcement from obtaining the court's authorization to delay notification of the Federal Express package search, even for a modest amount of time, potentially forcing investigators to choose between the credit card fraud and drug trafficking investigations. This is because investigators in this case obtained a delayed-notice search warrant only because immediate notice would have "seriously jeopardized" their drug investigation by, among other reasons, endangering their ongoing wiretap. This option, however, would no longer be available under the SAFE Act.

The Honorable Arlen Specter
Page 5

Contrary to concerns expressed by some, the "seriously jeopardize" prong is not used in run-of-the-mill cases. Indeed, the requirement that immediate notice result in "serious" jeopardy to an investigation would preclude its routine use. The Department estimates that fewer than one in 500 of the search warrants that have been obtained since the passage of the USA PATRIOT Act have been delayed-notice search warrants. In other words, in over 499 of 500 cases, immediate notice was provided. Moreover, approximately one in three delayed-notice search warrants obtained by the Department in the last two years relied on the fact that immediate notification would seriously jeopardize an investigation as the sole basis for delaying notice. Thus, fewer than one in 1500 search warrants relied solely on this prong of the statute.

Section 3 of the SAFE Act also would impose a seven-day limit on the initial period of delay regardless of the circumstances and would limit the period of delay under an extension to 21 days. In addition, requests for an extension would have to be approved by the Attorney General, Deputy Attorney General, or Associate Attorney General. Currently, under section 213 of the USA PATRIOT Act, the period of delay is set by the court and must be "reasonable" under the circumstances. Requiring the Government to go back to court after seven days -- even where the court would have found a longer period of delay reasonable -- would unnecessarily burden law enforcement and judicial resources. And although the provision for a 21-day extension period is less problematic than the 7-day period in the version of the SAFE Act introduced in the 108th Congress, requiring the Attorney General, Deputy Attorney General, or the Associate Attorney General (the three highest-ranking Justice Department officials) to personally certify extension requests would be unnecessarily burdensome and would divert resources from other necessary duties. Such a requirement should only be mandated in the exercise of extraordinary powers, and delayed-notice search warrants are a time-tested investigative tool that courts have repeatedly found to be consistent with the Fourth Amendment. Instead, the determination of what length of delay is reasonable should be made at the outset by a judge familiar with the particular investigation on a case-by-case basis, as is the case under existing law.

Section 4. Section 4 of the SAFE Act would deny terrorism investigators access to crucial intelligence information by: (1) raising the standard under which the FISA Court can order the production of business records and other tangible things; (2) restricting the types of business records that could be obtained through a section 215 order; (3) limiting the current nondisclosure requirement; (4) adding impracticable restrictions on the use of information obtained through section 215; and (5) imposing unworkable judicial review provisions. As previously announced by the Attorney General, the Department supports clarifying that the recipient of an order under section 215 may consult his attorney about the order and may seek judicial review of the production order in the FISA Court. However, the particular judicial review provisions in section 4 of the SAFE Act contain serious flaws -- for example, replacing the important presumption in favor of protecting classified national security information with a presumption in favor of disclosure. The additional amendments to section 215 the SAFE Act contemplates would render the tool essentially useless to investigators.

The Honorable Arlen Specter
Page 6

Section 4 would prevent the FISA Court from issuing an order under section 215 unless the Government provided "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 standard, which is higher than the standard under which Federal grand juries can subpoena the same records in ordinary criminal investigations, would effectively disable the Government from using a section 215 order to develop evidence at the early stages of an investigation, which is precisely when a section 215 order is the most useful. In addition, section 4 would prevent investigators from acquiring records that were indisputably relevant to an ongoing international terrorism or espionage investigation. Suppose, for example, investigators are surveilling a known al Qaeda operative and see him having dinner with three people, who split the check four ways and pay with credit cards. Investigators know nothing about the other people except they had dinner with an international terrorist, which would not constitute specific and articulable facts that each and every one of them is a terrorist. As an investigative matter, however, agents would like to know who they are. An easy way to do so would be to get a section 215 order for the credit card slips from the restaurant. While investigators could demonstrate that this information is relevant to the ongoing investigation (and thus meet the existing standard), they could not demonstrate sufficient specific and articulable facts that those individuals are agents of a foreign power, as section 4 would require. Raising the standard above relevance, and requiring 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" would render section 215 a dead letter.

The SAFE Act would provide for two general types of judicial review: review of motions brought by the recipient of a section 215 order, which could challenge either the order to produce records or the nondisclosure requirement that attaches to a section 215 order; and review of motions brought later by any "aggrieved person," defined as a person whose items or information were sought under section 215.

Although the Department has stated that it would support an amendment to allow the recipient of a section 215 order to challenge the production order pursuant to appropriate procedures in the FISA Court, the SAFE Act's provisions for such challenges are flawed and have the potential to cause risk to the national security. First, the SAFE Act would allow the recipient to challenge the order in either a United States District Court or the FISA Court. The Department could not support a provision allowing motions to be filed in a court other than the FISA Court, especially without a requirement that such filings be made under seal and be reviewed ex parte and in camera, because the FISA Court is better equipped to handle the sensitive, classified information at issue. Moreover, the FISA Court, with its particular expertise, is in a better position to assess the merits of a challenge to a section 215 order. Indeed, section 215 orders are issued by the FISA Court, and any motion to set aside or amend the order should be directed to the issuing court. Second, the SAFE Act would impose an automatic stay on the production order pending the resolution of the petition for review, which is unusual and would further undermine the Department's ability to obtain information in a timely manner.

The Honorable Arlen Specter
Page 7

Third, the SAFE Act would provide a strong presumption in favor of the disclosure of highly sensitive or classified materials including FISA Court applications, orders, and information obtained therefrom. When Congress enacted FISA in 1978, it recognized that the information involved in national security investigations must be safeguarded; it therefore provided statutory protections to that information in FISA itself. Section 4 of the SAFE Act would turn this statutory scheme on its head, requiring disclosure of portions of the 215 application, order, related materials, or derived evidence to the recipient or criminal defendant and/or his or her counsel, "unless the court finds that such disclosure would not assist in determining any legal or factual issue pertinent to the case." It is hard to imagine a circumstance in which information sought would not even "assist" the court in determining "any" legal or factual issue "pertinent" to the case. This strong presumption in favor of disclosure of classified information is completely unacceptable.

Section 4 would place investigators in the position of foregoing this valuable preliminary investigatory tool for fear of jeopardizing sensitive national security information. Suppose, for example, the information underlying the application came from a foreign government; if the foreign government knows that U.S. law contains a presumption of disclosure of this information to a petitioner (or a criminal defendant), the foreign government could decide not to share the information or to place restrictions on the use of the information. A dilemma would also arise if the source of the information in the application were a sensitive human source, who could be endangered through disclosure, leaving investigators with the choice of endangering the source or not obtaining the section 215 order. The presumption in favor of disclosure in litigation would inevitably have a negative impact on our ability to gather information about, and eventually prosecute individuals for, serious international terrorism and espionage-related crimes.

Section 4's provisions allowing an "aggrieved party" against whom section 215-derived information is later used to move to suppress that information in any civil or criminal proceeding is equally problematic and unnecessary. Third parties normally have no right to suppress information obtained from someone else. This, for example, is true in the case of grand jury subpoenas. *See, e.g., United States v. Miller*, 425 U.S. 435 (1976) (holding that bank customer had no standing to challenge the validity of grand jury subpoenas issued to a bank for his records). Similarly, a defendant in a criminal proceeding has no constitutional right to suppress evidence obtained in a search of someone else's property, even if that search was conducted unlawfully. *See, e.g., Rakas v. Illinois*, 439 U.S. 128 (1978) (passengers in car have no standing to suppress evidence obtained in allegedly illegal search and seizure of car); *see also Wong Sun v. United States*, 371 U.S. 471 (1963) (defendant may not suppress evidence obtained as a product of statement made by co-defendant incident to an unlawful arrest, even though the evidence was inadmissible against co-defendant); *United States v. Mendoza-Burciaga*, 981 F.2d 192 (5th Cir. 1992) (driver of a truck has standing to challenge a search of the truck, but a passenger does not). The proponents of the SAFE Act have not made a case for importing a novel third-party suppression remedy with respect to evidence obtained through section 215, which is an investigative tool similar to a grand jury subpoena and much less intrusive than a search.

The Honorable Arlen Specter
Page 8

The SAFE Act's suppression remedy also contains a presumption in favor of sharing highly sensitive national security information. Although existing law provides for the possibility that such information would have to be disclosed in a criminal procedure, the standard for disclosure is much higher. For example, the information must be exculpatory, or must *materially assist* preparation of the defense, as set forth in Rule 16 of the Federal Rules of Criminal Procedure. Under the SAFE Act, by contrast, information *shall* be disclosed unless "the court finds that such disclosure would not assist in determining *any* legal or factual issue *pertinent* to the case." (Emphasis added.) Under current law, no district court has ever ordered the Government to disclose even a portion of a FISA application; by contrast, the SAFE Act would place a heavy thumb on the side of disclosure. This section would also create an anomalous statutory regime where an individual challenging the minimally intrusive investigation technique of section 215 would have access to more FISA information than the target of a FISA search or surveillance.

Critically, the disclosure provisions are not limited to the criminal context, where a defendant's constitutional due process interest in receiving information must be afforded significant weight. The disclosure mechanism would also apply to a *civil* proceeding, such as one to amend or waive the nondisclosure requirement or to amend or quash the order itself. The SAFE Act purports to address the national security interests at stake by importing Classified Information Procedures Act ("CIPA") provisions to govern disclosure, but these provisions are inapposite. CIPA currently applies in the criminal context, to protect the due process rights of an accused, and relies on constitutional and statutory touchstones that apply only in the criminal context. The civil context simply does not function under the same rules, nor should it.

Section 4 also inappropriately places an artificial time limit on the nondisclosure requirement applying to the recipient, limiting the initial nondisclosure period to 180 days, which could be extended for an additional period of 180 days upon application by the Government. The burden would be on the Government in moving to extend the nondisclosure period, and in order to prevail, the Government would have to provide specific and articulable facts showing that disclosure "will result in - (A) endangering the life or physical safety of any person; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously endangering the national security of the United States by alerting a target, a target's associates, or the foreign power of which the target is an agent, of the Government's interest in the target." (Emphasis added). The FISA Court could issue an *ex parte* order extending the nondisclosure requirement only upon finding that one of the listed consequences "will" result. This provision sets an inappropriately high standard for maintaining the nondisclosure requirement and would thus make it far more difficult for investigators to safeguard important information. Section 4 also fails to recognize the extended nature of sensitive terrorism and espionage investigations. Such national security investigations do not typically end within six months, and many continue for a number of years. That is one reason why the current section 215 nondisclosure requirements are consistent with nondisclosure requirements concerning all methods of FISA surveillance, including far more intrusive means of surveillance. For example, a phone company is not permitted to tell a subscriber that his or her phone has been tapped pursuant to a FISA order.

The Honorable Arlen Specter
Page 9

Moreover, this provision would have the incongruous result of placing the burden on the Department to go to court repeatedly to extend nondisclosure requirements in sensitive terrorism and espionage investigations even when the recipient indicates no interest in disclosing information about the section 215 order.

Section 215's nondisclosure requirement not only serves to ensure that terrorists and spies are not tipped off that they are under investigation, it also serves to protect the privacy and reputation of individuals whose records are obtained by the Government under the provision. Suppose, for example, that the Department obtains the hotel records of an individual in a terrorism investigation but later is able to eliminate the individual in question from suspicion. Because of the nondisclosure requirement, the individual's connection to the investigation currently remains secret. Under the SAFE Act, however, the hotel would be free to publicize the name of the individual whose records were obtained in the terrorism investigation, thus running the risk that the individual's reputation would be ruined in the community.

The Department also would oppose the SAFE Act's limitations on use and disclosure of section 215-derived information. We know from experience with such limitations on information derived from more invasive investigative techniques such as electronic surveillance that, as a practical matter, the process for obtaining approval from the Attorney General to use FISA material in a criminal proceeding restricts the ability of prosecutors to use FISA information. Creating another category of materials that cannot be used on the criminal side of an investigation without explicit approval from the Attorney General when there are fewer equities involved that weigh in favor of imposing such a requirement would have a significantly detrimental effect on our ability to operate.

Finally, section 4 provides that even where the court finds that the section 215 order was lawfully issued, the court "may" (but is not required to) deny a motion challenging its legality. This provision, which appears to allow a court to second-guess the decision of the FISA Court to issue a section 215 order upon application by the Executive Branch even where the reviewing court has found the 215 order to be lawful would constitute unprecedented judicial interference with the conduct of foreign intelligence investigations.

The Government has used section 215 judiciously, and not once to obtain records from either a bookstore or a library between passage of the Act and March 30, 2005. In view of this responsible use and the utility of section 215 as a preliminary investigative tool, we could not support the radical changes the SAFE Act would work.

Section 5. Section 5 of the SAFE Act would impose entirely new restrictions on the use of national security letters ("NSLs"), making it more difficult to use this tool than it was prior to the USA PATRIOT Act. For years, Congress has authorized law enforcement to issue national security letters in very limited circumstances to obtain specific types of important information from certain third parties faster than they can with any other tool, while still allowing law enforcement to protect sensitive

The Honorable Arlen Specter
Page 10

information and ongoing investigations. The SAFE Act's proposed amendments relating to NSLs would resemble its amendments to section 215 orders, and would pose many of the same challenges as discussed above.

The SAFE Act would raise the standard for requesting information through an NSL, imposing a requirement that an NSL be supported by specific and articulable facts giving reason to believe that the records or information sought pertains to a foreign power or agent of a foreign power. In the case of communications providers, for example, section 215 would also require a showing of specific and articulable facts giving reason to believe "that communications facilities registered in the name of the person or entity have been used" in communication with "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities" involving a violation of criminal law, or with a foreign power or agent. Raising the standard in this way would prevent the Government from using these information requests at the beginning of investigations, precisely when they are most useful, just as section 4 would place cumbersome restraints on the use of section 215.

Section 5 would amend the current nondisclosure requirements relating to receipt by clarifying that a recipient could disclose receipt to obtain legal advice and to comply with such a request. The Department has previously taken the position in litigation that the NSL statutes already permit the recipient of an NSL to consult with his or her attorney. However, the provision also would limit to 90 days the nondisclosure period attaching to an NSL, after which the burden would be on the Government to seek extensions in 180-day increments to prevent a recipient from disclosing receipt not just to counsel or to persons necessary for compliance, but to anyone, including the target of an investigation. As with the proposed amendments to section 215, we could not support placing the burden on the Government each and every time to justify why highly sensitive national security information should be kept secret.

The judicial review provisions of section 5 mirror those set forth in section 4 and are equally flawed. As is the case with the SAFE Act's amendments to section 215, section 5 of the SAFE Act provides one general procedure for judicial review of several types of pleadings in both the civil and criminal contexts. The provision is particularly confusing when applied to NSLs because it refers to a requirement that the court shall disclose, pursuant to CIPA, "portions of the *application, order, or other related materials unless the court finds that such disclosure would not assist in determining any legal or factual issue pertinent to the case.*" (Emphasis added.) However, there is no requirement that the Government apply for or receive a court order prior to issuing an NSL. Moreover, as discussed above, CIPA procedures simply would be inapposite in the context of a civil proceeding to set aside or modify either the production request or nondisclosure requirement.

Section 6. Section 6 would make it more difficult to obtain a pen register or trap and trace device in the criminal investigative context than it was before the enactment of the USA PATRIOT Act. This section would require investigators to provide the court with "specific and articulable facts showing there is reason to believe" the information to be obtained via the pen register or trap and trace device

The Honorable Arlen Specter

Page 11

would be relevant to an ongoing criminal investigation, which is a standard much closer to probable cause. Existing law in both the FISA and criminal investigative contexts currently requires a Government certification of relevance. This lower threshold is appropriate for pen registers and trap and trace devices, which are investigative tools less intrusive than searches or electronic surveillance, and often are used early in an investigation to obtain evidence that will serve as the building blocks of an investigation and may later support the probable cause showing required to obtain court approval to use those more intrusive investigative means. Indeed, existing law, which requires pen registers and trap and trace devices to be authorized by a judge, provides more protection than is constitutionally required, as the Supreme Court has held that no court approval is constitutionally necessary to install or use a pen register or trap and trace device. *Smith v. Maryland*, 442 U.S. 735, 744 (1979). By raising the standard for these devices to specific and articulable facts in both the FISA and criminal investigative contexts, it will be much harder for investigators to use a valuable tool, thus hampering intelligence and criminal investigations.

The SAFE Act also would add a notice requirement to section 3123 of title 18. Current law provides that a pen register order shall "be sealed until otherwise ordered by the court." Pursuant to the proposal, however, the court that receives an application or extension request *shall* serve on the persons named in the application and such other parties to communications as the court determines should receive notice in the interest of justice, an inventory within a specified time period. The inventory would include the fact of the application or extension request and whether it was granted or denied. If the application or extension request were granted, the inventory would also include the date of entry and period of authorized or unauthorized use; whether the device was installed or used; and the specific types of dialing, routing, addressing, or signaling information sought and collected. Finally, the court could make available such specified information to a person served with such an inventory, including portions of the collected communications, applications, and orders, as the court determined to be in the interest of justice.

Although section 6 provides for a delay of notice, because of the number of pen registers and traps/traces being conducted, this could prove to be a monumental task for some of the larger offices that are actively involved in these types of investigations. The dialing, routing, addressing, and signaling information obtained through a pen register can be obtained by an administrative subpoena, and is, at best, minimally intrusive on a person's right to privacy. Notification to the persons listed in the pen register/trap application would only serve to alert them to the fact that law enforcement is conducting an investigation of their criminal behavior, thus allowing them to avoid potential arrest and prosecution by changing their methods of operation. Investigations are seldom completed and at the stage where notification could be appropriate after only 90 days. As such, notice could endanger human lives when an undercover agent and/or an informant are involved with the target.

In similar circumstances in the Title III context, the Electronic Surveillance Unit of the Office of Enforcement Operations has had several instances in terrorism investigations where they were ready to send the cases forward for approval by the Office of the Assistant Attorney General for the Criminal

The Honorable Arlen Specter
Page 12

Division, prior to an application to the court for a Title III order, where either the FBI or the Counterterrorism Section of the Criminal Division determined that it could not risk the chance that the wiretap would be disclosed within 90 days should a judge not agree that good cause existed to delay the inventory notice. If that has been the concern in wiretap investigations, the problem would multiply exponentially in cases where the law required 90-day notification to the targets and/or subscribers of numbers obtained pursuant to pen register and trap and trace devices. It is hard to imagine the resources that would be necessary in order to provide timely notice relating to the countless non-pertinent phone numbers identified by pen registers and trap and trace devices during the course of one year, should "such other parties to communications as the court determines should receive notice in the interest of justice" be interpreted by courts to include all of the persons whose phone numbers were revealed in connection with a pen/trap order.

Section 7. The Department opposes the modification to the definition of domestic terrorism in section 7 of the SAFE Act. Were this section to be enacted into law, many violent and deadly activities undertaken with a terrorist intent would no longer fall under the definition of domestic terrorism.

Under current law, domestic terrorism consists of activities that: (1) involve acts dangerous to human life that (2) are a violation of State or Federal criminal law and (3) appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping. In addition, such acts must occur primarily within the territorial jurisdiction of the United States. *See* 18 U.S.C. § 2331(5). As a result, an activity cannot qualify as an act of domestic terrorism unless it both endangers human life and constitutes a criminal offense. In addition, it is important to recognize that, like the statutory definition of "international terrorism," *see* 18 U.S.C. § 2331(1), the definition of "domestic terrorism" does not criminalize any conduct, but is used only in conjunction with other statutory provisions. For example, a multidistrict search warrant authorized under Rule 41(a) of the Federal Rules of Civil Procedure may be issued in an investigation of "domestic terrorism," and information obtained through a criminal investigative wiretap about potential acts of "domestic terrorism" may be shared with appropriate Federal, State, local, and foreign government officials.

Section 7 of the SAFE Act would redefine the term "domestic terrorism" to include only acts dangerous to human life that constitute a specified "Federal crime of terrorism," *see* 18 U.S.C. § 2332b(g)(5), that occur primarily within the territorial jurisdiction of the United States. This provision, however, would create large gaps in the definition of domestic terrorism. For example, were a domestic terrorist, such as a violent white supremacist, to assassinate a State governor (or even five State governors simultaneously), this would no longer be considered an act of "domestic terrorism" were the SAFE Act to be enacted into law. Moreover, violent and deadly acts perpetrated by ecoterrorists would no longer fall under the definition of that term. Such acts may qualify as domestic terrorism where they are designed to intimidate or coerce a civilian population by forcing individuals or companies to change their behavior. Ecoterrorists, for example, have burned down homes and businesses in order to deter developers from contributing to "sprawl." Such actions, however, would

The Honorable Arlen Specter
Page 13

not fall within the SAFE Act's definition of domestic terrorism. This is because, among other reasons, under the Act's definition, the requisite terrorist intent would have to involve an attempt to influence, affect, or retaliate against government conduct, and would no longer include the intent to intimidate or coerce a civilian population. Compare 18 U.S.C. § 2332b(g)(5)(A), with 18 U.S.C. § 2331(5)(B).

In justifying section 7 of the SAFE Act, proponents have voiced the concern that peaceful political protestors currently may be labeled as domestic terrorists; this concern, however, is unfounded. Peaceful political protest is not an activity that is "dangerous to human life" and thus would not fall within the current definition of "domestic terrorism." In addition, Federal law already defines "domestic terrorism" in a narrower manner than it does "international terrorism." International terrorism, for example, consists of violent acts *and* acts dangerous to human life, while the definition of domestic terrorism includes only those actions that endanger human life. For these reasons, the Department does not believe that it is necessary to amend the current definition of "domestic terrorism."

Section 8. The Department strongly opposes the modification of current reporting requirements concerning the use of FISA authorities and opinions of the FISA Court set forth in section 8 of the SAFE Act. Were this provision to be adopted, it would unwisely restrict the ability of the Department to provide Congress with information in a manner that protects national security.

In addition to other significant reporting requirements currently placed upon the Department with respect to FISA authorities, *see, e.g.*, 50 U.S.C. § 1808, section 6602 of the Intelligence Reform and Terrorism Prevention Act of 2004 imposed a new reporting requirement. Under this provision, the Attorney General must report to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the committees on the Judiciary of the House of Representatives and the Senate on a semiannual basis a variety of information, including: (1) the aggregate number of persons targeted under FISA for electronic surveillance, physical searches, pen registers, and access to records; (2) the number of times that the Attorney General has authorized the use of information obtained under FISA, or any information derived therefrom, in a criminal proceeding; (3) a summary of significant legal interpretations of FISA involving matters before the FISA Court or FISA Court of Review contained in applications or pleadings filed with those courts by the Department of Justice; and (4) copies of all decisions and opinions of the those courts including significant construction or interpretation of FISA.

Significantly, the Attorney General is allowed to transmit this sensitive information to Congress "in a manner consistent with the protection of national security." The SAFE Act, however, would remove the provision allowing for the transmission of this information in a manner consistent with the protection of national security. Moreover, it actually would require the Department to make this information public, subject only to the qualification that the Department would be allowed to redact decisions and opinions of the FISA Court and FISA Court of Review in order to protect national security. This qualification, however, is plainly insufficient because other public disclosures mandated by section 8 would be very damaging to national security.

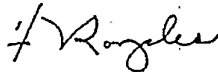
The Honorable Arlen Specter
Page 14

The Department of Justice currently complies with its obligation to fully inform appropriate congressional committees regarding its use of FISA authorities, which allows them to perform their critical oversight functions. The Department, however, cannot support any expansion of these reporting requirements that would restrict the ability of the Department to transmit information to Congress in a manner consistent with the protection of national security. Moreover, the Department is unable to support any proposal that would require the public disclosure of sensitive information. As the SAFE Act would have precisely that effect, the Department does not support section 8. To give just one specific example, significant legal interpretations of FISA may involve the application of the Act to a particular surveillance technique or circumstance confronted by agents. While currently the Department is required to present, in a manner consistent with national security, a summary of such interpretations to specified congressional committees, under the SAFE Act that summary would have to be provided to the public. Such a public report, however, could jeopardize national security as interpretations as to how FISA applies to a particular surveillance technique or circumstance confronted by investigators could provide terrorists or spies with tools and guidance for avoiding surveillance.

The Department of Justice believes that the SAFE Act, which would significantly modify some of the USA PATRIOT Act's most valuable provisions and, in some ways, would make it more difficult to protect Americans than before the USA PATRIOT Act, must be rejected. The ongoing congressional hearings on the USA PATRIOT Act make clear the importance of that law in preserving our ability to protect Americans and the values we all cherish; the SAFE Act would unnecessarily place the Department's capacity to safeguard the safety and security of the American people at risk.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,



Alberto R. Gonzales
Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

184

ENCLOSURE 3

EFF Section 215-794

207 27 2004 9 2007

11/05 P 3

~~SECRET~~

General Donald J. Ryder

b6 -1,2
b7C -1,2

SA [redacted] asked what had happened to cause the detainee to grimace in pain. The witness said [redacted] had grabbed the detainee's thumbs and beat them backwards and indicated that she also grabbed his genitals. The witness also implied that her treatment of the detainee was less harsh than her treatment of others by indicating that he had seen her treatment of other detainees result in detainees coming into a fetal position on the floor and crying in pain.

b6 -1,2,5
b7C -1,2,5

2. Also in October 2002, FBI Special Agent [redacted] was observing the interrogation of a detainee while [redacted] a civilian contractor, came up the observation screen and asked SA [redacted] to come see something. SA [redacted] then pulled the curtain behind the observation screen in another interrogation room. SA [redacted] asked Mr. [redacted] whether the detainee had spit at the interrogators. Mr. [redacted] laughed and stated that the detainee had been shouting the Quran and would not stop. Mr. [redacted] did not observe when SA [redacted] asked [redacted]

b6 -4
b7C -4

3. In September or October of 2002 FBI agents observed that a detainee was treated in an aggressive manner to intimidate detainees. [redacted] had, in November 2002, FBI agents observed [redacted] after he had been subjected to intense isolation for over three months. During that time period [redacted] was totally isolated (with the exception of occasional interrogations) in a cell that was always flooded with light. By late November, the detainee was evidencing behavior consistent with extreme psychological trauma (talking to non-existent people, reporting hearing voices, crouching in a corner of the cell covered with a sheet for hours on end). It is unknown to the FBI whether such extended isolation was approved by appropriate DoD authorities.

These situations were referenced in a May 30, 2003 electronic communication (EC) from the Behavioral Analysis Unit of the FBI to FBI Headquarters. That EC attached, among other documents, a Report Memorandum for the Record dated 15 January 2003 from Capt. [redacted] (USAFR), that refers to the first two events among others in a time line of events related to discussions concerning the use of aggressive interrogation techniques. Marian Bowman of the FBI's Office of General Counsel discussed the contents of these communications with Mr. Dietz, Deputy General Counsel (Intelligence) and Mr. De'Orto, Deputy General Counsel of DoD, around the time the EC was received. Although he was assured that the general concerns expressed and the debate between the FBI and DoD regarding the treatment of detainees was known to officials in the Pentagon, I have no record that our specific concerns regarding these three situations were communicated to DoD for appropriate action.

b6 -2
b7C -2

DETAINEES-3824

~~SECRET~~

OCT 27 2004 5 25AM

~~SECRET~~

General Donald J. Ryder

If I can provide any further information to you, please do not hesitate to call.

Sincerely yours,

T. J. Herington
Deputy Assistant Director
Computer/Network Division

DETAINEE-3825

3.

~~SECRET~~

~~SECRET~~

188

ENCLOSURE 4

EFF Section 215-798

Requested by SSA [REDACTED] FBI (SAL) at Guantanamo Bay and forwarded to Marion Bowman, Legal Counsel, FBIHQ, on 1/27/2002.

LEGAL ANALYSIS OF INTERROGATION TECHNIQUES:

Interrogation Techniques

Category I--

1. Gagging with gauze.
2. Yelling at detainee.
3. Deception
 - a. Multiple interrogators
 - b. Interrogator posing as an interrogator from a foreign nation with a reputation of harsh treatment of detainees.

Category II--

1. Use of stress positions (such as standing) for a maximum of 4 hrs.
2. Use of falsified documents or reports.
3. Isolation facility for 30 day increments.
4. Non-standard interrogation environment/booth.
5. Humiliating detainee.
6. Use of 20-hour interrogation segments.
7. Removal of all comfort items (including religious items).
8. Switching detainee from hot rations to MRE's.
9. Removal of all clothing.
10. Forced grooming (shaving of facial hair etc...)
11. Use of individual phobias (such as fear of dogs) to induce stress.

Category III--

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
3. Use of wet towel and dripping water to induce the misperception of drowning.
4. Use of mild physical contact such as grabbing, light pushing and poking with finger.

Category IV--

1. Detainee will be sent off GTMO, either temporarily or permanently, to Jordan, Egypt, or another third country to allow those countries to employ interrogation techniques that will enable them to obtain the requisite information.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED

Legal Analysis

The following techniques are examples of coercive interrogation techniques which are not permitted by the U.S. Constitution:

Category I -

3. b. Interrogator posing as an interrogator from a foreign nation with a reputation of harsh treatment of detainees.

Category II -

1. Use of stress positions (such as standing) for a maximum of 4 hrs.
2. Use of falsified documents or reports.
5. Hooding detainee.
6. Use of 20-hour interrogation segments.
9. Removal of all clothing.
11. Use of individual phobias (such as fear of dogs) to induce stress.

Category III -

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
3. Use of wet towel and dripping water to induce the misperception of drowning.

Information obtained through these methods will not be admissible in any Criminal Trial in the U.S. Although, information obtained through these methods might be admissible in Military Commission cases, the Judge and or Panel may determine that little or no weight should be given to information that is obtained under duress.

The following techniques are examples of coercive interrogation techniques which may violate 18 U.S.C. s. 2340, (Torture Statute):

Category II -

5. Hooding detainee.
11. Use of individual phobias (such as fear of dogs) to induce stress.

Category III -

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
4. Use of wet towel and dripping water to induce the misperception of drowning.

In 18 U.S.C. s. 2340, (Torture Statute), torture is defined as "an act committed by a person acting under color of law specifically intended to inflict severe physical or mental pain or suffering upon another person within his custody or control." The torture statute defines "severe mental pain or suffering" as "the prolonged mental harm caused by or resulting from the intentional infliction or threatened infliction of severe physical pain or suffering; or the administration or application, or threatened administration or application, of mind-altering substances or other procedures calculated to disrupt profoundly the senses of the personality; or the threat of imminent death; or the threat that another person will imminently be subject to death, severe physical pain or suffering, or the administration or application, of mind-altering substances or other procedures calculated to disrupt profoundly the senses of the personality."

Although the above interrogation techniques may not be per se violations of the United States Torture Statute, the determination of whether any particular use of these techniques is a violation of this statute will hinge on the intent of the user. The intent of the user will be a question of fact for the Judge or Jury to decide. Therefore, it is possible that those who employ these techniques may be indicted, prosecuted, and possibly convicted if the trier of fact determines that the user had the requisite intent. Under these circumstances it is recommended that these techniques not be utilized.

The following technique is an example of a coercive interrogation technique which appears to violate 18 U.S.C. s. 2340, (Torture Statute):

Category IV-

1. Detainee will be sent off GTMO, either temporarily or permanently, to Jordan, Egypt, or another third country to allow those countries to employ interrogation techniques that will enable them to obtain the requisite information.

In as much as the intent of this category is to utilize, outside the U.S., interrogation techniques which would violate 18 U.S.C. s. 2340 if committed in the U.S., it is a per se violation of the U.S. Torture Statute. Discussing any plan which includes this category, could be seen as a conspiracy to violate 18 U.S.C. s. 2340. Any person who takes any action in furtherance of implementing such a plan, would incipate all persons who were involved in creating this plan. This technique can not be utilized without violating U. S. Federal law.

SUBMISSIONS FOR THE RECORD



News From: _____

U.S. Senator Russ Feingold

506 Hart Senate Office Building
Washington, D.C. 20510-4904
(202) 224-5323

<http://www.senate.gov/~feingold>

Contact: Zach Lowe
(202) 224-0981

Statement of Senator Russ Feingold
Senate Judiciary Committee Hearing
On "Oversight of the USA PATRIOT Act"

April 5, 2005

Mr. Chairman, thank you very much for holding this hearing today. I am pleased that we are beginning our review of the PATRIOT Act early in the year, and I thank you for your commitment to taking the time necessary to review the Executive Branch's exercise of government power since September 11.

The PATRIOT Act was proposed just days after the horrific September 11th attacks, and the bill was passed and signed into law just a little more than a month later. I tried at that emotionally charged time to convince my colleagues that some provisions went too far and needed to be revised, including the business records authority in Section 215, but my amendments were rejected – although, Mr. Chairman, I want to note for the record that you supported me in some of those efforts, and I do appreciate that.

I voted against the PATRIOT Act, but I am heartened that now, four years later, as some provisions are up for reauthorization, Congress will have the time and perspective that we didn't have then to carefully and calmly consider these expanded government powers. As the Justice Department has correctly argued, some of the expiring provisions are not especially controversial, and I suspect we will be able to conclude quickly that they should be reauthorized with no changes. Other provisions of the Patriot Act, however, including some provisions *not* subject to the sunset, deserve close scrutiny. Some may require modification to ensure adequate protection of civil liberties going forward.

I have introduced a number of bills to modify the PATRIOT Act. In addition, along with several members of this Committee, I have supported Senator Craig's and Senator Durbin's SAFE Act, which offers reasonable accountability mechanisms to ensure adequate oversight of the Executive Branch as it engages in the very important and difficult work of protecting us from terrorist attacks. I want to emphasize, Mr. Chairman, that I do not believe we should repeal the PATRIOT Act. But we do have the

1600 Aspen Commons
Middleton, WI 53562
(608) 828-1200

517 E. Wisconsin Ave.
Milwaukee, WI 53202
(414) 276-7282

First Star Plaza
401 5th St., Room 410
Wausau, WI 54403
(715) 846-5660

425 State St., Room 232
La Crosse, WI 54603
(608) 782-5585

121 Main Street
Green Bay, WI 54302
(920) 465-7508

EFF Section
215-858

responsibility, as the 9-11 Commission noted in its recommendation, to provide adequate safeguards to govern the use of executive powers, which I think we failed to do when we passed the PATRIOT Act.

I also want to emphasize that there are a variety of other civil liberties issues, beyond those arising directly from the PATRIOT Act, that warrant intense congressional scrutiny and oversight this year. I look forward to working with you, Mr. Chairman, with Attorney General Gonzales and Director Mueller, and with other members of the Committee as we embark on the reauthorization process.



Department of Justice

STATEMENT

OF

ALBERTO R. GONZALES
ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

THE USA PATRIOT ACT

PRESENTED ON

APRIL 5, 2005

**STATEMENT OF ALBERTO R. GONZALES
ATTORNEY GENERAL OF THE UNITED STATES
BEFORE THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
APRIL 5, 2005**

Chairman Specter, Ranking Member Leahy, and Members of the Committee:

It is my pleasure to appear before you this morning to discuss the USA PATRIOT Act. Approximately three-and-a-half years ago, our Nation suffered a great tragedy. Thousands of our fellow citizens were murdered at the World Trade Center, the Pentagon, and a field in rural Pennsylvania. We will never forget that day or the heroes who perished on that hallowed ground. Forever in our Nation's collective memory are stories of the New York City firefighters who rushed into burning buildings so that others might live and of the brave passengers who brought down United Airlines Flight 93 before it could reach Washington, DC, and the messages from those trapped in the World Trade Center saying their last goodbyes to loved ones as they faced certain death will stay forever in our hearts.

In the wake of this horrific attack on American soil, we mourned our Nation's terrible loss. In addition, we came together in an effort to prevent such a tragedy from ever happening again. Members of both parties worked together on legislation to ensure that investigators and prosecutors would have the tools they need to uncover and disrupt terrorist plots. Additionally, members joined hands across the aisle to guarantee that our efforts to update and strengthen the laws governing the investigation and prosecution of terrorism remained firmly within the parameters of the Constitution and our fundamental national commitment to the protection of civil rights and civil liberties.

The result of this collaboration was the USA PATRIOT Act, which passed both Houses of the Congress with overwhelming bipartisan majorities and was signed into law by President Bush on October 26, 2001. In the past three-and-a-half years, the USA PATRIOT Act has been an integral part of the Federal Government's successful prosecution of the war against terrorism. 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.

Many of the most important provisions of the USA PATRIOT Act, however, are scheduled to expire at the end of this year. Therefore, I am here today primarily to convey one simple message: All provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year must be made permanent. While we have made considerable progress in the war against terrorism in the past three-and-a-half years, al Qaeda and other terrorist groups still pose a grave threat to the safety and security of the American people. The tools contained in the USA PATRIOT Act have proven to be essential weapons in our arsenal to combat the terrorists, and now is not the time for us to be engaging in unilateral disarmament. Moreover, many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as was intended by Congress, not only in terrorism cases, but also to combat other serious criminal conduct. If these provisions are not renewed, the Department's ability to combat serious offenses such as cybercrime, child pornography, and kidnappings will also be hindered.

As Congress considers whether to renew key USA PATRIOT Act provisions, I also wish to stress that I am open to any ideas that may be offered for improving these

provisions. If members of this Committee or other members of Congress wish to offer proposals in this regard, I and others at the Department of Justice would be happy to consult with you and review your ideas. However, let me be clear about one thing: I will not support any proposal that would undermine the ability of investigators and prosecutors to disrupt terrorist plots and combat terrorism effectively.

It is also my sincere hope that we will be able to consider these crucial issues in a calm and thoughtful fashion. All of us seek to ensure the safety and security of the American people and to protect their civil liberties as well. As this debate goes forward, I will treat those who express concerns about the USA PATRIOT Act with respect and listen to their concerns with an open mind. I also hope that all who participate in the debate will stick to the facts and avoid overheated rhetoric that inevitably tends to obfuscate rather than elucidate the truth.

Today, I would like to use the rest of my testimony to explain how key provisions of the USA PATRIOT Act have helped to protect the American people. I will particularly focus on those sections of the Act that are scheduled to expire at the end of 2005. To begin with, I will discuss how the USA PATRIOT Act has enhanced the federal government's ability to share intelligence. Then, I will explain how the USA PATRIOT Act provided terrorism investigators with many of the same tools long available to investigators in traditional criminal cases. Additionally, I will explore how the USA PATRIOT Act updated the law to reflect new technology. And finally, I will review how the Act protects the civil liberties of the American people and respects the important role of checks and balances within the Federal Government.

Information Sharing

The most important reforms contained in the USA PATRIOT Act improved coordination and information sharing within the Federal Government. Prior to the attacks of September 11, 2001, our counterterrorism efforts were severely hampered by unnecessary obstacles and barriers to information sharing. These obstacles and barriers, taken together, have been described as a "wall" that largely separated intelligence personnel from law enforcement personnel, thus dramatically hampering the Department's ability to detect and disrupt terrorist plots.

It is vitally important for this Committee to understand how the "wall" was developed and how it was dismantled, not for the purpose of placing blame but rather to ensure that it is never rebuilt. Before the passage of the USA PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA) mandated that applications for orders authorizing electronic surveillance or physical searches under FISA were required to include a certification that "the purpose" of the surveillance or search was to gather foreign intelligence information. This requirement, however, came to be interpreted by the courts and later the Department of Justice to require that the "primary purpose" of the collection was to obtain foreign intelligence information rather than evidence of a crime. And, because the courts evaluated the Department's purpose for using FISA, in part, by examining the nature and extent of coordination between intelligence and law enforcement personnel, 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, a finding that would prevent the court from authorizing surveillance under FISA. As a result, over the years, the "primary purpose"

standard had the effect of constructing a metaphorical "wall" between intelligence and law enforcement personnel.

During the 1980s, a set of largely unwritten rules only limited information sharing between intelligence and law enforcement officials to some degree. In 1995, however, the Department established formal procedures that limited the sharing of information between intelligence and law enforcement personnel. 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.

As they were originally designed, 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 surveillance and later use the fruits of that surveillance 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 permitted in theory. Due both to the complexities of the restrictions on information sharing and to a perception that improper information sharing could end a career, investigators often erred on the side of caution and refrained from sharing information. The end result was a culture within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

In hindsight, it is difficult to overemphasize the negative impact of the "wall." In order to uncover terrorist plots, it is essential that investigators have access to as much information as possible. Often, only by piecing together disparate and seemingly

unrelated points of information are investigators able to detect suspicious patterns of activity, a phenomenon generally referred to as "connecting the dots." If, however, one set of investigators has access to only one-half of the dots, and another set of investigators has access to the other half of the dots, the likelihood that either set of investigators will be able to connect the dots is significantly reduced.

The operation of the "wall" was vividly illustrated in testimony from Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, before the Senate Judiciary Committee:

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."

Thanks in large part to the USA PATRIOT Act, this "wall" has been lowered. 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 foreign-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.

Section 218 of the USA PATRIOT Act not only removed what was perceived at the time as the primary impediment to robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing. Thanks to the USA PATRIOT Act, the Department has been able to move from a culture where information sharing was viewed with a wary eye to one where it is an integral component of our counterterrorism strategy. Following passage of the Act, the Department adopted new procedures specifically designed to increase information sharing between intelligence and law enforcement personnel. Moreover, Attorney General Ashcroft instructed every U.S. Attorney across the country to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. He also directed every U.S. Attorney to develop a plan to monitor intelligence investigations, to ensure that information about terrorist threats is shared with other agencies, and to consider criminal charges in those investigations.

The increased information sharing facilitated by section 218 of 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 four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen 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 I am not at liberty to discuss today.

While the "wall" primarily blocked the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often prevented 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 are 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, to support the revocation of suspected terrorists' visas, to track terrorists' funding sources, and to identify terrorist operatives overseas.

The information sharing provisions described above have been heralded by investigators in the field as the most important provisions of the USA PATRIOT Act. Their value has also been recognized by the 9/11 Commission, which stated in its official report that "[t]he provisions in the act that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial."

Since the passage of the USA PATRIOT Act, Congress has taken in the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 other important steps forward to improve coordination and information sharing throughout the Federal Government. If Congress does not act by the end of the year, however, we will soon take a dramatic step back to the days when unnecessary obstacles blocked vital information sharing. Three of the key information sharing provisions of the USA PATRIOT Act, sections 203(b), 203(d), and 218, are scheduled to sunset at the end of the year. It is imperative that we not allow this to happen. To ensure that the "wall" is not reconstructed and investigators are able to "connect the dots" to prevent future terrorist attacks, these provisions must be made permanent.

Using Preexisting Tools in Terrorism Investigations

In addition to enhancing the information sharing capabilities of the Department, the USA PATRIOT Act also permitted several existing investigative tools that had been used for years in a wide range of criminal investigations to be used in terrorism cases as

well. Essentially, these provisions gave investigators the ability to fight terrorism utilizing many of the same court-approved tools that have been used successfully and constitutionally for many years in drug, fraud, and organized crime cases.

Section 201 of the USA PATRIOT Act is one such provision. In the context of criminal law enforcement, Federal investigators have long been able to obtain court orders to conduct wiretaps when investigating numerous traditional criminal offenses. Specifically, these orders have authorized the interception of certain communications to investigate the predicate offenses listed in the federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses include numerous crimes, such as drug crimes, mail fraud, passport fraud, embezzlement from pension and welfare funds, the transmission of wagering information, and obscenity offenses.

Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit were not included in this list, which prevented law enforcement authorities from using wiretaps to investigate these serious terrorism-related offenses. As a result, law enforcement could obtain under appropriate circumstances a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into terrorism transcending national boundaries.

Section 201 of the Act ended this anomaly in the law by amending the criminal wiretap statute to add the following terrorism-related crimes to the list of wiretap predicates: (1) chemical-weapons offenses; (2) certain homicides and other acts of violence against Americans occurring outside of the country; (3) the use of weapons of mass destruction; (4) acts of terrorism transcending national borders; (5) financial

transactions with countries which support terrorism; and (6) material support of terrorists and terrorist organizations.

This provision simply enables investigators to use wiretaps when looking into the full range of terrorism-related crimes. This authority makes as much, if not more, sense in the war against terrorism as it does in traditional criminal investigations; if wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national borders, chemical weapons offenses, and other serious crimes that terrorists are likely to commit.

It is also important to point out that section 201 preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 206 of the USA PATRIOT Act, like section 201 discussed above, provided terrorism investigators with an authority that investigators have long possessed in traditional criminal investigations. Before the passage of the Act, multipoint or so-called "roving" wiretap orders, which attach to a particular suspect rather than a particular phone or communications facility, were not available under FISA. As a result, each time an international terrorist or spy switched communications providers, for

example, by changing cell phones or Internet accounts, investigators had to return to court to obtain a new surveillance order, often leaving investigators unable to monitor key conversations.

Congress eliminated this problem with respect to traditional criminal crimes, such as drug offenses and racketeering, in 1986 when it authorized the use of multi-point or "roving" wiretaps in criminal investigations. But from 1986 until the passage of the USA PATRIOT Act in 2001, such authority was not available under FISA for cases involving terrorists and spies. Multi-point wiretaps could be used to conduct surveillance of drug dealers but not international terrorists. However, such authority was needed under FISA. International terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making vital the ability to obtain "roving" surveillance. Without such surveillance, investigators were often left two steps behind sophisticated terrorists.

Section 206 of the Act amended the law to allow the FISA Court to authorize multi-point surveillance of a terrorist or spy when it finds that the target's actions may thwart the identification of those specific individuals or companies, such as communications providers, whose assistance may be needed to carry out the surveillance. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other "specified person" whose assistance may be required.

A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that multi-point wiretaps are perfectly consistent with the Fourth Amendment. Section 206 simply authorizes the same constitutional techniques used to

investigate ordinary crimes to be used in national-security investigations. Despite this fact, section 206 remains one of the more controversial provisions of the USA PATRIOT Act. However, as in the case of multi-point wiretaps used for traditional criminal investigations, section 206 contains ample safeguards to protect the privacy of innocent Americans.

First, section 206 did not change FISA's requirement that the target of multi-point surveillance must be identified or described in the order. In fact, section 206 is always connected to a particular target of surveillance. For example, even if the Justice Department is not sure of the actual identity of the target of such a wiretap, FISA nonetheless requires our attorneys to provide a description of the target of the electronic surveillance to the FISA Court prior to obtaining multi-point surveillance order.

Second, just as the law required prior to the Act, the FISA Court must find that there is probable cause to believe the target of surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. In addition, the FISA Court must also find that the actions of the target of the application may have the effect of thwarting surveillance before multi-point surveillance may be authorized.

Third, section 206 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Section 214 is yet another provision of the USA PATRIOT Act that provides terrorism investigators with the same authority that investigators have long possessed in traditional criminal investigations. Specifically, this section allows the government to obtain a pen register or trap-and-trace order in national security investigations where the

information to be obtained is likely to be relevant to an international terrorism or espionage investigation. A pen register or trap-and-trace device can track routing and addressing information about a communication – for example, which numbers are dialed from a particular telephone. Such devices, however, are not used to collect the content of communications.

Under FISA, intelligence officers may seek a court order for a pen register or trap-and-trace to gather foreign intelligence information or information about international terrorism. Prior to the enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought to obtain with a pen register or trap-and-trace device would be relevant to their investigation, but also that the particular facilities being monitored, such as phones, were being used by foreign governments, international terrorists, or spies. As a result, it was much more difficult to obtain a pen register or trap-and-trace device order under FISA than it was under the criminal wiretap statute, where the applicable standard was and remains simply one of relevance in an ongoing criminal investigation.

Section 214 of the Act simply harmonized the standard for obtaining a pen register order in a criminal investigation and a national-security investigation by eliminating the restriction limiting FISA pen register and trap-and-trace orders to facilities used by foreign agents or agents of foreign powers. Applicants must still, however, certify that a pen register or trap-and-trace device is likely to reveal information relevant to an international terrorism or espionage investigation or foreign intelligence information not concerning a United States person. This provision made the standard contained in FISA for obtaining a pen register or trap-and-trace order parallel with the

standard for obtaining those same orders in the criminal context. Now, as before, investigators cannot install a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court.

I will now turn to section 215, which I recognize has become the most controversial provision in the USA PATRIOT Act. This provision, however, simply granted national security investigators the same authority that criminal investigators have had for centuries – that is, to request the production of records that may be relevant to their investigation. For years, ordinary grand juries have issued subpoenas to obtain records from third parties that are relevant to criminal inquiries. But just as prosecutors need to obtain such records in order to advance traditional criminal investigations, so, too, must investigators in international terrorism and espionage cases have the ability, with appropriate safeguards, to request the production of relevant records.

While obtaining business records is a long-standing law enforcement tactic that has been considered an ordinary tool in criminal investigations, prior to the USA PATRIOT Act it was difficult for investigators to obtain access to the same types of records in connection with foreign intelligence investigations. Such records, for example, could be sought only from common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. In addition, intelligence investigators had to meet a higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation.

To address this anomaly in the law, section 215 of the Act made several important changes to the FISA business-records authority so that intelligence agents would be better

able to obtain crucial information in important national-security investigations. Section 215 expanded the types of entities that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The new provision contains no such restrictions. Section 215 also 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)."

I recognize that section 215 has been subject to a great deal of criticism because of its speculative application to libraries, and based on what some have said about the provision, I can understand why many Americans would be concerned. The government should not be obtaining the library records of law-abiding Americans, and I will do everything within my power to ensure that this will not happen on my watch.

Section 215 does not focus on libraries. Indeed, the USA PATRIOT Act nowhere mentions the word "library," a fact that many Americans are surprised to learn. Section 215 simply does not exempt libraries from the range of entities that may be required to produce records. Now some have suggested, since the Department has no interest in the reading habits of law-abiding Americans, that section 215 should be amended to forbid us from using the provision to request the production of records from libraries and booksellers. This, however, would be a serious mistake.

Libraries are currently not safe havens for criminals. Grand jury subpoenas have long been used to obtain relevant records from libraries and bookstores in criminal investigations. In fact, law enforcement used this authority in investigating the Gianni

Versace murder case as well as the case of the Zodiac gunman in order to determine who checked out particular books from public libraries that were relevant in those murder investigations. And if libraries are not safe havens for common criminals, neither should they be safe havens for international terrorists or spies, especially since we know that terrorists and spies have used libraries to plan and carry out activities that threaten our national security. The Justice Department, for instance, has confirmed that, as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.

Section 215, moreover, contains very specific safeguards in order to ensure that the privacy of law-abiding Americans, both with respect to their library records as well as other types of records, is respected. First, section 215 expressly protects First Amendment rights, unlike grand jury subpoenas. Even though libraries and bookstores are not specifically mentioned in the provision, section 215 does prohibit the government from using this authority to conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." In other words, the library habits of ordinary Americans are of no interest to those conducting terrorism investigations, nor are they permitted to be.

Second, any request for the production of records under section 215 must be issued through a court order. Therefore, investigators cannot use this authority unilaterally to compel any entity to turn over its records; rather, a judge must first approve the government's request. By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval. Both grand jury subpoenas and section

215 orders are also governed by a standard of relevance. Under section 215, agents may not seek records that are irrelevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Third, section 215 has a narrow scope. It can only be used in an authorized investigation (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. On the other hand, a grand jury may obtain business records in investigations of *any* federal crime.

Finally, section 215 provides for thorough congressional oversight that is not present with respect to grand-jury subpoenas. On a semi-annual basis, I must "fully inform" appropriate congressional committees concerning all requests for records under section 215 as well as the number of section 215 orders granted, modified, or denied. To date, the Department has provided Congress with six reports regarding its use of section 215.

Admittedly, the recipient of an order under section 215 is not permitted to make that order publicly known, and this confidentiality requirement has generated some fear among the public. It is critical, however, that terrorists are not tipped off prematurely about sensitive investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government's investigation has been completed. As the U.S. Senate concluded when adopting FISA: "By its very nature, foreign intelligence surveillance must be conducted in secret."

Updating the Law To Reflect New Technology

As well as providing terrorism investigators many of the same tools that law enforcement investigators had long possessed in traditional criminal investigations, many sections of the USA PATRIOT Act updated the law to reflect new technology and to prevent sophisticated terrorists and criminals from exploiting that new technology. Several of these provisions, some of which are currently set to sunset at the end of this year, simply updated tools available to law enforcement in the context of ordinary criminal investigations to address recent technological developments, while others sought to make existing criminal statutes technology-neutral. I wish to focus on five such provisions of the Act, which are currently set to expire at the end of 2005. The Department believes that each of these provisions has proven valuable and should be made permanent.

Section 212 amended the Electronic Communications Privacy Act to authorize electronic communications service providers to disclose communications and records relating to customers or subscribers in an emergency involving the immediate danger of death or serious physical injury. Before the USA PATRIOT Act, for example, if an Internet service provider had learned that a customer was about to commit a terrorist act and notified law enforcement to that effect, the service provider could have been subject to civil lawsuits. Now, however, providers are permitted voluntarily to turn over information to the government in emergencies without fear of civil liability. It is important to point out that they are under no obligation whatsoever to review customer communications and records. This provision also corrected an anomaly in prior law under which an Internet service provider could voluntarily disclose the content of

communications to protect itself against hacking, but could not voluntarily disclose customer records for the same purpose.

Communications providers have relied upon section 212 to disclose vital and time-sensitive information to the government on many occasions since the passage of the USA PATRIOT Act, thus saving lives. To give just one example, this provision was used to apprehend an individual threatening to destroy a Texas mosque before he could carry out his threat. Jared Bjarnason, a 30-year-old resident of El Paso, Texas, sent an e-mail message to the El Paso Islamic Center on April 18, 2004, threatening to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Section 212 allowed FBI officers investigating the threat to obtain information quickly from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could attack the mosque. It is not clear, however, that absent section 212 investigators would have been able to locate and apprehend Bjarnason in time.

Section 212 of the USA PATRIOT Act governed both the voluntary disclosure of the content of communications and the voluntary disclosure of non-content customer records in emergency situations; but in 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision that is not scheduled to sunset. The remaining portion of section 212, governing the disclosure of customer records, however, is set to expire at the end of 2005. Should section 212 expire, communications providers would be able to disclose the content of customers' communications in emergency situations but would not be able voluntarily to disclose

non-content customer records pertaining to those communications. Such an outcome would defy common sense. Allowing section 212 to expire, moreover, would dramatically restrict communications providers' ability voluntarily to disclose life-saving information to the government in emergency situations.

Section 202, for its part, modernized the criminal code in light of the increased importance of telecommunications and digital communications. The provision allows law enforcement to use pre-existing wiretap authorities to intercept voice communications, such as telephone conversations, in the interception of felony offenses under the Computer Fraud and Abuse Act. These include many important cybercrime and cyberterrorism offenses, such as computer espionage and intentionally damaging a Federal Government computer. Significantly, section 202 preserved all of the pre-existing standards in the wiretap statute, meaning that law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, as was the case prior to the passage of the USA PATRIOT Act, then surely investigators should be able to use them when investigating computer espionage, extortion, and other serious cybercrime and cyberterrorism offenses.

Turning to section 220, that provision allows courts, in investigations over which they have jurisdiction, to issue search warrants for electronic evidence stored outside of the district where they are located. Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old. Prior to the USA PATRIOT Act, some courts interpreting Rule 41 of the Federal Rules of Criminal Procedure declined to issue search warrants for e-mail messages stored on servers in other districts, leading to delays in many time-sensitive investigations as investigators had to bring agents, prosecutors, and judges in another district up to speed. Requiring investigators to obtain warrants in distant jurisdictions also placed enormous administrative burdens on districts in which major Internet service providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a murder investigation in Pennsylvania can issue a search warrant for e-mail messages pertaining to that investigation that were stored on a server in Silicon Valley. Thus, investigators in Pennsylvania, under this scenario, can ask a judge familiar with the investigation to issue the warrant rather than having to ask Assistant United States Attorneys in California, who are unfamiliar with the case, to ask a judge in the United States District Court for the Northern District of California, who is also unfamiliar with the case, to issue the warrant.

The Department has already utilized section 220 in important terrorism investigations. As Assistant Attorney General Christopher Wray testified before this committee on October 21, 2003, section 220 was useful in the Portland terror cell case

because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This section has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist Richard Reid. Moreover, the ability to obtain search warrants in the jurisdiction of the investigation has proven critical to the success of complex, multi-jurisdictional child pornography cases.

Contrary to concerns voiced by some, section 220 does not promote forum-shopping; the provision may be used only in a court with jurisdiction over the investigation. Investigators may not ask any court in the country to issue a warrant to obtain electronic evidence.

It is imperative that section 220 be renewed; allowing the provision to expire would delay many time-sensitive investigations and result in the inefficient use of investigators', prosecutors', and judges' time.

Moving to section 209, that provision made existing statutes technology-neutral by providing that voicemail messages stored with a third-party provider should be treated like e-mail messages and answering machine messages, which may be obtained through a search warrant. Previously, such messages fell under the rubric of the more restrictive provisions of the criminal wiretap statute, which apply to the interception of live conversations. Given that stored voice communications possess few of the sensitivities associated with the real-time interception of telephone communications, it was unreasonable to subject attempts to retrieve voice-mail message stored with third-party

providers to the same burdensome process as requests for wiretaps. Section 209 simply allows investigators, upon a showing of probable cause, to apply for and receive a court-ordered search warrant to obtain voicemails held by a third-party provider, preserving all of the pre-existing standards for the availability of search warrants. Since the passage of the USA PATRIOT Act, such search warrants have been used in a variety of criminal cases to obtain key evidence, including voicemail messages left for foreign and domestic terrorists, and to investigate a large-scale Ecstasy smuggling ring based in the Netherlands.

The speed with which voicemail is seized and searched can often be critical to an investigation given that deleted messages are lost forever. Allowing section 209 to expire, as it is set to do in 2005, would once again require different treatment for stored voicemail messages than for messages stored on an answering machine in a person's home, needlessly hampering law enforcement efforts to investigate crimes and obtain evidence in a timely manner.

Section 217 similarly makes criminal law technology-neutral, placing cyber-trespassers on the same footing as physical intruders by allowing victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now invite law enforcement assistance to assist them in combating cyber-intruders. Section 217 does not require computer operators to involve law enforcement if they detect trespassers on their systems; it simply gives them the option to do so. In so doing, section 217 also preserves the privacy of law-abiding computer users by sharply limiting the circumstances under

which section 217 is available. Officers may not agree to help a computer owner unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will not acquire the communications of non-trespassers. Moreover, the provision amended the wiretap statute to protect the privacy of an Internet service provider's customers by providing a definition of "computer trespasser" which excludes an individual who has a contractual relationship with the service provider. Therefore, for example, section 217 would not allow Earthlink to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers.

Since its enactment, section 217 has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. Section 217 is also particularly helpful when computer hackers launch massive "denial of service" attacks – which are designed to shut down individual web sites, computer networks, or even the entire Internet. Allowing section 217 to expire, which is set to occur in 2005, would lead to a bizarre world in which a computer hacker's supposed privacy right would trump the legitimate privacy rights of a hacker's victims, making it more difficult to combat hacking and cyberterrorism effectively.

Protecting Civil Liberties

While the USA PATRIOT Act provided investigators and prosecutors with tools critical for protecting the American people, it is vital to note that it did so in a manner fully consistent with constitutional rights of the American people. In section 102 of the USA PATRIOT Act, Congress expressed its sense that "the civil rights and civil liberties of all Americans . . . must be protected," and the USA PATRIOT Act does just that.

In the first place, the USA PATRIOT Act contains several provisions specifically designed to provide additional protection to the civil rights and civil liberties of all Americans. Section 223, for example, allows individuals aggrieved by any willful violation of the criminal wiretap statute (Title III), the Electronic Communications Privacy Act, or certain provisions the FISA, to file an action in United States District Court to recover not less than \$10,000 in damages. This provision allows an individual whose privacy is violated to sue the United States for money damages if Federal officers or employees disclose sensitive information without lawful authorization. Section 223 also requires Federal departments and agencies to initiate a proceeding to determine whether disciplinary action is warranted against an officer or employee whenever a court or agency finds that the circumstances surrounding a violation of Title III raise serious questions about whether that officer or employee willfully or intentionally violated Title III. To date, there have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the USA PATRIOT Act. I believe that this reflects the fact that employees of the Justice Department consistently strive to comply with their legal obligations. Nevertheless, section 223 provides an important mechanism for holding the Department of Justice accountable, and I strongly urge Congress not to allow it to sunset at the end of 2005.

Additionally, section 1001 of the USA PATRIOT Act requires the Justice Department's Inspector General to designate one official responsible for the review of complaints alleging abuses of civil rights and civil liberties by Justice Department employees. This individual is then responsible for conducting a public awareness campaign through the Internet, radio, television, and newspaper advertisements to ensure

that individuals know how to file complaints with the Office of the Inspector General. Section 1001 also directs the Office of Inspector General to submit to this Committee and the House Judiciary Committee on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by Department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General pursuant to section 1001; they were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. I am pleased to be able to state that the Office of the Inspector General has not documented in these reports any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the USA PATRIOT Act.

In addition to containing special provisions designed to ensure that the civil rights and civil liberties of the American people are respected, the USA PATRIOT Act also respects the vital role of the judiciary by providing for ample judicial oversight to guarantee that the constitutional rights of all Americans are safeguarded and that the important role of checks and balances within our Federal Government is preserved. As reviewed above, under section 214 of the Act, investigators cannot utilize a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court. Section 215 of the Act requires investigators to obtain a court order to request the production of business records in national security investigations. Section 206 requires the Foreign Intelligence Surveillance Court to approve the use of "roving" surveillance in national security investigations. Sections 201 and 202 require a Federal court to approve the use of a criminal investigative wiretap, and sections 209 and 220 require a Federal court to issue search warrants to obtain evidence in a criminal investigation.

Besides safeguarding the vital role of the judiciary, the USA PATRIOT Act also recognizes the crucial importance of congressional oversight. On a semiannual basis, for example, as noted before, I am required to report to this Committee and the House Judiciary Committee the number of applications made for orders requiring the production of business records under section 215 as well as the number of such orders granted, modified or denied. I am also required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on a semiannual basis concerning all requests for the production of business records under section 215. These reports were transmitted by the Department to the appropriate committees in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004. Moreover, I am required by statute to submit a comprehensive report on a semiannual basis to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of FISA. These reports contain valuable information concerning the Department's use of USA PATRIOT Act provisions, including sections 207, 214, and 218.

Finally, I would note that the Department has gone to great lengths to respond to congressional concerns about the implementation of the USA PATRIOT Act. The Department has, for example, provided answers to more than 520 oversight questions from Members of Congress regarding the USA PATRIOT Act. In the 108th Congress alone, in fact, the Department sent 100 letters to Congress that specifically addressed the USA PATRIOT Act. The Department also has provided witnesses at over 50 terrorism-related hearings, and its employees have conducted numerous formal and informal

briefings with Members and staff on USA PATRIOT Act provisions. In short, the Department has been responsive and will continue to be responsive as Congress considers whether key sections of the USA PATRIOT Act will be made permanent.

Conclusion

In closing, the issues that we are discussing today are absolutely critical to our Nation's future success in the war against terrorism. The USA PATRIOT Act has a proven record of success when it comes to protecting the safety and security of the American people, and we cannot afford to allow many of the Act's most important provisions to expire at the end of the year. For while we certainly wish that the terrorist threat would disappear on December 31, 2005, we all know that this will not be the case. I look forward to working with the Members of this Committee closely in the weeks and months ahead, listening to your concerns, and joining together again on a bipartisan basis to ensure that those in the field have the tools that they need to effectively prosecute the war against terrorism. I also look forward to answering your questions today.

STATEMENT OF SENATOR CHARLES GRASSLEY
UNITED STATES SENATE JUDICIARY COMMITTEE
"OVERSIGHT OF THE USA PATRIOT ACT"

APRIL 5, 2005

Mr. Chairman, thank you for scheduling this oversight hearing on the PATRIOT Act. As you may know, I have resisted efforts to make changes to the Act before it was ripe for review. Now is that time, and I'm glad we have this opportunity to discuss how effective the Act has been and if provisions of the Act need to be modified. It would also be appropriate to discuss any proposed expansion of the Act.

I appreciate Attorney General Gonzales and Director Mueller making themselves available to answer our questions. With sixteen provisions of the PATRIOT Act sunseting at the end of the year, it is fitting that the AG and FBI Director explain how these provisions have been helpful in the war against terror.

In 2001, I supported the PATRIOT Act, because I believed it provided the right balance between assisting our law enforcement agencies with the means to combat terror while also protecting the civil liberties that we Americans hold so dear. The Act struck this important balance, giving federal authorities more effective tools to fight terrorism. The Attorney General said it well in a speech before the National Association of Counties, "without security, government cannot deliver, nor can the people enjoy, the prosperity and opportunities that flow from freedom and democracy."

Now that it is time to consider renewing the provisions of the Act that are about to sunset, we should remember that the Act has been instrumental in helping Federal authorities thwart terrorist activities since September 11, 2001. The Act has been critical to our war on terror because it made two fundamental changes to the way we do business. First, the Act tore down the wall that prevented federal law enforcement and the intelligence community from sharing information regarding terrorists. The 9/11 Commission highlighted the ill advised nature of a system where communications between agents conducting intelligence investigations and the criminal prosecution units at the Department of Justice were prevented.

The second change was updating the surveillance tools used by federal investigators in terrorism cases. We must remember that the surveillance statutes updated by the PATRIOT Act had been enacted decades ago when the rotary telephone was the primary communications technology. In some traditional criminal areas, the federal courts had sanctioned the use of new surveillance tools. In fact, many of the tools addressed in the PATRIOT Act have been in use for years in drug trafficking, child pornography, and white collar fraud cases. It made no sense that federal law enforcement investigators would be able to use these tools in those criminal cases, but not in the war against terror. The PATRIOT Act changed this, giving federal investigators tools appropriate for the 21st century. These two changes have resulted in a more secure America, so we should think long and hard before we decide not to renew them.

In the three and a half years since the PATRIOT Act was enacted, there have been numerous terrorism-related prosecutions resulting in convictions. Virtually all of the actions taken by the Federal government under the PATRIOT Act have been reviewed by independent Federal judges with no provision in the Act being successfully challenged in federal court.

Frankly, any discussion of renewing the PATRIOT Act's surveillance provisions must of necessity include talking about oversight of the Act. Where the Congress has expanded the government's authorities to conduct surveillance, it is inherent that the Congress makes sure that the government has not misused that authority. So it is my position that any bill regarding the PATRIOT Act include adequate oversight and reporting measures. Chairman Specter, Senator Leahy, and I introduced a bill last Congress, the "Domestic Surveillance Oversight Act," to allow Congress and the public to better monitor the terrorism investigations of federal agencies. This was an important piece of legislation that should be added to any bill to renew and/or revise the PATRIOT Act.

Additionally, I am particularly proud of two legislative initiatives which I co-authored that were a part of the PATRIOT Act. Those legislative efforts helped law enforcement officials identify and detect the transfer of illicit funds by international criminals through the banking system. These provisions have helped to shut off the spigot that allows tainted money to flow through the U.S. banking system and finance terrorist activities in the United States and around the world. As the Senate considers renewal of the PATRIOT Act, I will be taking the opportunity to also discuss my Combating Terrorist Financing and Money Laundering bill. Although the Committee was unable to consider my bill during last Congress, I hope that it will be enacted this year.

Further, I am concerned about the working relationship between the FBI and other law enforcement agencies on terrorists financing investigations. In early 2003, as the Department of Homeland Security (DHS) had just begun operation, Secretary Ridge and Attorney General Ashcroft signed a Memorandum of Agreement (MOA) which terminated Operation Green Quest and transferred lead responsibility and control of all terrorist financing investigations to the FBI. Operation Green Quest began shortly after the 9/11 attacks and was transferred from the Customs Service to Immigration and Customs Enforcement (ICE) when DHS was created. By all accounts, it was a major success, yielding 38 arrests, 26 indictments, and the seizure of \$6.8 million in terrorist assets in its first nine months of existence. Yet, the FBI succeeded in killing the program and ensuring that no similar initiative could be started by ICE in the future.

The MOA represented a significant victory for the FBI in the turf battle surrounding the creation of DHS. In theory, the MOA is supposed to preserve "the significant expertise and capabilities of ICE" in terrorist financing investigations. However, I understand that the way this MOA is being implemented and enforced has created a disincentive in the field for ICE agents to focus their efforts on investigations related to terrorist financing. I know of at least one instance, for example, where ICE spent significant resources pursuing an investigation and coordinating with the FBI every step of the way, only to have FBI headquarters use the MOA to step-in at the last minute, demand control of the investigation, and unnecessarily delay a critical wiretap request. This delay may well have prevented the collection of vitally important information related to terrorist financing, and for what purpose? So, that the FBI can protect its turf?

I have also heard that this is not an isolated incident, that there may be other cases involving similar turf problems. Congress needs to take a hard look at this MOA and the way the FBI is enforcing it. Is it necessary to ensure a unified approach to terrorist financing investigations? Or does it simply serve to protect the interest of the FBI in expanding its own jurisdiction? As Chair of the Finance Committee, I am particularly interested in making sure that the elements of the Treasury Department, ICE, and the FBI are all working together smoothly to stop terrorist financing activity, not battling each other for jurisdiction. Therefore, I intend to inquire about some of these cases in the coming weeks. I hope that Attorney General Gonzales and Director Mueller will welcome an honest look at these questions and cooperate fully with requests for information on these issues.

Mr. Chairman, I once again want to thank you for holding today's hearing, and of course I want to express my gratitude to the Attorney General and Director Mueller for their willingness to answer our questions today.

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, COMMITTEE ON THE JUDICIARY
HEARING ON OVERSIGHT OF THE USA PATRIOT ACT
APRIL 5, 2005

On a September morning three and one-half years ago nearly three thousand lives were lost on American soil, and our lives as Americans changed in an instant. In the aftermath of the 9/11 attacks, Congress moved quickly -- some have said too quickly -- to give federal authorities substantial new powers to investigate and prosecute terrorism. The USA PATRIOT Act, a landmark and sweeping measure, was signed into law on October 30, 2001, just six weeks after the attacks.

Some of us sitting here today contributed to the PATRIOT Act. We worked together in a bipartisan manner, and with common resolve to craft a bill that we hoped would make us safer as a Nation. Freedom and security are always in tension in our society, but we tried our best to strike the right balance. Now it is time to return to this discussion to assess what aspects we got right and what modifications need to be made.

I negotiated many of the provisions of the PATRIOT Act and am gratified to have been able to add several checks and balances that were not in the initial proposal. The White House reneged on some agreements that we had mutually reached to strike a better balance on some of the PATRIOT Act's provisions. It is also true that additional checks and balances that I and others sought, had the White House agreed to them, would have yielded the same benefits to our law enforcement efforts, but with greater accountability and less opportunity for abuse. In the final negotiating session, former House Majority Leader Dick Armey and I insisted that we add a sunset for certain governmental powers that have great potential to affect the civil liberties of the American people. That sunset provision is the reason we are here today. It ensured that we would revisit the PATRIOT Act and shine some sunlight on how it has been implemented.

As we all know, the vast majority of the provisions of the PATRIOT Act are not subject to sunset. Of the handful that will expire at the end of the year, some are non-controversial and can be renewed with little or no modification. Others require greater scrutiny. For example, many of us have expressed concerns with the business records subpoena power in section 215, and its implications for libraries and booksellers. I have cosponsored legislation, introduced by Senator Feingold, that addresses this provision.

Before we rush to renew any controversial powers created by the PATRIOT Act, we need to understand how these powers have been used, and whether they have been effective. A few weeks ago, we celebrated the first National Sunshine Week with a hearing on open

government and bipartisan calls for responsiveness and accountability. We should carry that theme into this process of oversight and legislating.

We should also bear in mind the 9/11 Commission's counsel about the PATRIOT Act. They wrote, "The burden of proof for retaining a particular governmental power should be on the Executive, to explain (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."

We are in a new Congress with a new Chairman of this Committee. Chairman Specter has a distinguished record as a steadfast advocate and practitioner of meaningful oversight. We have before us a new Attorney General who has pledged to work with us on a number of issues, including the PATRIOT Act. The American people deserve to be represented by a Congress that takes its oversight responsibilities seriously, just as they deserve to see federal agencies cooperate with Congress. The breakdown of cooperation following passage of the PATRIOT Act has fostered distrust. We can change that by working together to achieve the right balance in our anti-terrorism laws, and then by allowing appropriate sunshine to illuminate the ways those laws are being used.

I just said that the new Chairman supports vigorous oversight. I am pleased that he has agreed to hold hearings on a number of important issues that fall under this Committee's jurisdiction. We will hold another hearing on the PATRIOT Act next month, to hear the views of experts from outside the government. Later this month, the Committee will hold a hearing -- the first of several, I hope -- to focus attention on the data brokering industry and its implications for individual privacy and government accountability. And finally, our new Chairman has expressed serious interest in holding a hearing that I have been requesting for more than a year, to examine the FBI's foreign language translation program. We are working together to schedule that event.

We have heard over and over again that there have been no abuses as a result of the PATRIOT Act. But it is difficult, if not impossible, to verify that claim when some of the most controversial surveillance powers in the PATRIOT Act operate under a cloak of secrecy. We know the government is using its surveillance powers under the Foreign Intelligence Surveillance Act more than ever, but everything else about FISA is secret. This difficulty in assessing PATRIOT's impact on civil liberties has been exacerbated greatly by the Administration's obstruction of legitimate oversight efforts.

Whether or not there have been abuses under the PATRIOT Act, the unchecked growth of secret surveillance powers and technologies with no real oversight by the Congress or the courts has resulted in clear abuses by the Executive Branch. We have seen secret arrests and secret hearings of hundreds of people for the first time in U.S. history; detentions without charges and denial of access to counsel; misapplication of the material witness statute as a sort of general preventive detention law; discriminatory targeting of Arabs and Muslims; selective enforcement of the immigration laws; and the documented mistreatment of aliens held on immigration charges. Such abuses harm our national security as well as civil liberties because they serve as recruiting posters for terrorists,

intimidate American communities from cooperating with law enforcement agencies and, by misusing limited anti-terrorism resources, make it more likely that real terrorists will escape detection.

Beyond this, the Administration has used brutal and degrading interrogation techniques against detainees in Afghanistan, Iraq, and Guantanamo Bay that run counter to past American military traditions, practices and ideals. Information about these disgraceful acts continues to trickle out in large part because of a persistent press and the results of a lawsuit filed under the Freedom of Information Act, or FOIA. Meanwhile, the Administration continues to stonewall, releasing information only when it is self-serving to do so, or when ordered to do so by the courts.

The Department of Justice has been particularly obstinate in its refusal to release information. Justice Louis Brandeis said, "Sunshine is the best disinfectant." But despite its claims that the Department of Justice redacts information only to protect national security and privacy, DOJ held back a considerable amount of potentially embarrassing information when it released FBI email traffic last December in response to the FOIA lawsuit. Some of these documents are several pages in length, yet are entirely redacted.

Two weeks ago, Senator Levin released a more complete version of one of these documents. What DOJ had originally refused to release were conclusions by federal agents at Guantanamo that the military interrogations were producing intelligence information that was "suspect as best." DOJ also redacted an assertion that the interrogation practices could undermine future military trials. Finally, DOJ blacked out a segment of the memo describing how its own Criminal Division lawyers took their concerns about the harsh interrogation techniques at Guantanamo to the Pentagon's General Counsel. Why would this piece of information be redacted? Perhaps because the Pentagon's General Counsel, William J. Haynes, is currently a nominee to the Fourth Circuit Court of Appeals. Mr. Haynes's nomination has become embroiled over concerns that he was deeply involved in developing the military's interrogation policies.

Finally, in yet another example of abuse, recent press reports provide disturbing details about how the Administration embraced the use of extraordinary rendition after the 9/11 attacks. Several press reports detail the CIA's use of jets to secretly transfer detainees to countries around the world, where it is likely that they will be tortured.

In defending the Administration's rendition policy, the President said in his March 17 press conference that, "we seek assurances that nobody will be tortured when we render a person back to their home country." This statement came only 10 days after Attorney General Gonzales acknowledged that we "can't fully control" what happens to detainees transferred to other nations, and added that he does not know whether countries have always complied with their promises.

I have introduced legislation that would end this abhorrent practice without expanding our obligations under the Convention Against Torture. It simply closes the loopholes in the Convention's implementing legislation, thus ensuring that we honor our commitment not to outsource torture to other countries.

These cases of overreaching and abuse trickled down from policy decisions that were made at the top. There will always be scandals and tragedies in a nation's history. What makes America special is that we do not hide from our mistakes; we investigate them, learn from them, and make sure they do not happen again. When necessary, we change our laws to reflect the lessons we have learned. The spirit of openness and accountability are what bring us here today to reconsider portions the PATRIOT Act. I welcome our witnesses and look forward to a fruitful discussion.

####



U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

The Honorable Richard B. Cheney
President of the Senate
United States Senate
Washington, D.C. 20510

Dear Mr. President:

This report is submitted pursuant to the Foreign Intelligence Surveillance Act of 1978, Title 50, United States Code, Section 1807, as amended.

During calendar year 2004, 1,758¹ applications were made to the Foreign Intelligence Surveillance Court for electronic surveillance and physical search. The 1,758 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search simultaneously. The Court approved 1,754 applications.

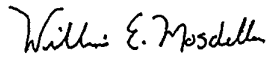
The Government withdrew three of the 1,758 applications made to the Court prior to the Court ruling on the applications. The Government later resubmitted one of the three applications, which was approved by the Court as a new application. The Court did not deny, in whole or in part, any application submitted by the Government in 2004.

Section 1807 also requires that the Government report, in addition to the number of applications approved or denied, the number of applications modified by the Court. During calendar

¹ One application, which is reflected in the 1758 applications made to the Court, was approved in 2003 and received a docket number in 2004.

year 2004, the Court made substantive modifications to the Government's proposed orders in 94 applications presented to the Court.

Sincerely,



William E. Moschella
Assistant Attorney General



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Pursuant to Section 2006 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458), enclosed please find the Department's report on translation services of the Federal Bureau of Investigation and other Department components for calendar year 2004. Please note that, in some instances, the report includes information in fiscal year terms because it is maintained on that basis.

We hope that this report is helpful. Please do not hesitate to contact this office if you would like additional assistance regarding any other matter.

Sincerely,

A handwritten signature in cursive script that reads "William E. Moschella".

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Report on Department of Justice Use of Translators

Pursuant to Section 2006 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458), the Attorney General submits the following report to the Committees on the Judiciary of the Senate and the House of Representatives on the use of translators by the United States Department of Justice.

1. The number of translators employed, or contracted for, by the FBI or other components of Department of Justice.

Breakdown Across Department

The following table provides a breakdown for components of the Department of Justice of (1) the number of translators employed as of January 2005 under authorized staffing levels for Fiscal Year 2005 (10/1/04 – 9/30/05); and (2) an estimated number of contract translators that will be utilized during Fiscal Year 2005, or that were used in Fiscal Year 2004, as explained in the notes following the chart. The Executive Office for Immigration Review (EOIR), United States Attorney's Offices (USA), the Criminal Division (CRM), and the Bureau of Prisons (BOP) use contract translators or interpreters, but those components are unable to estimate the number used. For these components, the chart refers to the notes for information regarding the use of contractor translators or interpreters.

<i>Department of Justice Translators by Component</i>	<i>Number of Federal Employees</i>	<i>Number of Contractors</i>
<i>Law Enforcement and Corrections</i>		
FBI	413	898
DEA	0	2,004
ATF	0	0
AFF	0	0
USMS	0	0
BOP	0	(See note)
USPC	0	5
ODT	0	0
Interpol	2	0
<i>Subtotal, Law Enforcement and Corrections</i>	415	2,907
<i>Litigating</i>		
ATR	0	1
CRM	0	(See note)
CIV	2	0
CRT	0	0
USA	2	(See note)
<i>Subtotal, Litigating</i>	4	1

<i>Adjudications</i>		
EOIR	101	(See note)
<i>Subtotal, Adjudications</i>	101	0
TOTAL, Department of Justice	520	2,908

CHART NOTES

The Federal Bureau of Investigation (FBI) translator program, involving both employees and contractors, is explained in detail in the subsection following these notes.

EOIR uses the services of contract interpreters, and estimates that these contractors will work 165,827 hours in FY 2005, the cost of which is estimated to be \$18,089,435. Since many of these contract interpreters may only work for a few hours, it is not possible to estimate the number working at any given time. The contractor has a roster of approximately 3,000 available interpreter subcontractors. Both the contract interpreters and the federal employees listed above for EOIR work with EOIR's Court Interpreter Program, where they interpret oral statements made in statements before immigration judges.

The Drug Enforcement Administration (DEA) notes that the number of contract linguists is an estimate and that contract linguist support varies depending on investigative requirements.

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) does not have full time translators or contractors. ATF does expend funds for translation services that usually entail audio tape translation and transcription and sometimes translation of printed documents of evidentiary value and pay foreign language bonuses to agents proficient in foreign languages. ATF anticipates awarding 107 foreign language bonuses to employees in FY 2005, totaling \$280,000. The bonus is paid to an employee who passes a proficiency test and makes substantial use of one or more foreign languages in the performance of his or her official duties for a substantial percent of his or her time on the job (10% of basic work schedule).

The Criminal Division (CRM) does not hire translators as employees nor do they have contractors on staff. However, the Division does have contracts with companies that provide translator service. The contractors do not perform their services within the Division; the documents requiring translation are sent to translators and the contractors send them back.

The U.S. Attorneys (USAs) note that there is a subclassification code in the Department's Financial Management Information System for Stenographic and Interpreter Services. In FY 2004, USAs paid \$5.8 million for these services. Unfortunately, there is no way to identify how much was for stenographic versus Interpreter Services. Also, there is no way to identify the number of people performing these services and/or how many are full time or part time.

Like the USAs, the BOP notes that it does use contract interpreters when needed in its prisons, but is unable to identify the number used. BOP has budgeted \$50,000 for contractor interpreters in FY 2005.

The Civil Division (CIV) has two people employed with the Office of Immigration

Litigation who perform translating services as well as other duties.

The United States National Central Bureau (USNCB) notes that the official working languages of the Interpol organization are French, English, Spanish and Arabic. Each Interpol member country is required to be able to communicate in writing in the four official languages. In order to meet this mandate the USNCB employs two full time translators. Both translators are proficient in English, French and Spanish. The majority of the Arab speaking countries communicate within the organization in the English language. In the past the USNCB has used contracted translators for Arabic translations.

In FY 2004, the United States Parole Commission spent around \$3,000 for the 5 contractors included above, all employed on various occasions.

The U.S. Marshals Service (USMS) confirmed that it has no translators, either federal employees or contractors. If the USMS needs something translated, it relies on the services of other agencies or task force participants (e.g., OCEETF and Fugitive Apprehension Teams).

The Assets Forfeiture Fund (AFF), the Office of Detention Trustee (ODT), the Civil Rights Division (CRT) and the Antitrust Division (ATR) do not use translators, either federal employees or contractors.

Breakdown of FBI Translators

The FBI has the most substantial translator program within the Department. The FBI uses a combination of Language Specialists (LS) and Contract Linguists (CL) to address its foreign language translation requirements. LSs are full-time salaried employees of the FBI, while CLs are self-employed contractors who work on an hourly basis. By relying on both full-time LSs and part-time CLs, the FBI is afforded maximum workforce flexibility in a fluid and shifting operating environment.

The following tables identify the FBI's current staffing as of January 4, 2005, and net growth in several critical languages:

FBI Linguists (Selected Critical Languages)					
Language	Linguists Approved for Access to Law Enforcement Sensitive (LES) and National Security Information (NSI)			ALL	% Growth
	Pre-9/11/01	LES	NSI		
Arabic	70	19	211	230	228.57%
Farsi	24	0	60	60	150%
Pashto	1	0	8	8	700%
Urdu	6	1	19	20	233.33%
Chinese	67	22	122	144	114.92%
French	16	6	30	36	125%
Hebrew	4	0	13	13	225%
Hindi	4	0	8	8	100%

Japanese	13	1	15	16	23.08%
Korean	18	2	26	28	55.56%
Kurdish	0	0	8	8	N/a
Russian	78	12	87	99	26.92%
Turkish	2	3	13	16	700%
Vietnamese	12	4	21	25	108.33%
All Languages	405 CLs; 379 LSs	898 CLs; 413 LSs			67.22%

2. Any legal or practical impediments using translators employed by the Federal, State or local agencies on a full-time, part-time or shared basis.

There are no legal impediments to using linguists from other federal, state or local agencies to augment FBI language resources. However, the practical impediments based on the scarcity of qualified translators available to the FBI and other federal agencies, particularly among Middle Eastern and Asian languages, have been well documented through Congressionally-sanctioned commission and GAO studies.¹ Since demand for translator resources in foreign languages within law enforcement agencies with the greatest translation needs is currently well in excess of supply, the concept of sharing translators is often impracticable given each agency's requirements for these limited resources. Such sharing is sometimes further complicated by non-uniform proficiency testing and clearance requirements throughout the federal government. Nevertheless, such sharing and pooling occurs regularly, usually between the FBI and agencies in the intelligence community, particularly in response to urgent operational needs.

Intelligence and Federal Law Enforcement Community

The intermediate and long-range benefits of pooling Intelligence Community (IC) translator resources are clear. Benefits would be even greater if each IC agency were provided sufficient resources to conduct aggressive recruitment and processing of translators and to develop those translators through language training. Otherwise, scarcity issues will continue to pose barriers to translator sharing.

The benefits of pooling federal law enforcement translator resources are not as clear. The reason is that such pooling does not always work when the receiving agency has higher vetting and clearance standards than the sharing agency. For example, the FBI's current excess supply of Spanish Contract Linguist resources could be used immediately by DEA, Customs, or ATF because of the higher vetting and clearance standards used by the FBI to meet its responsibilities relating to national security matters. However, it would often prove difficult to work in reverse since most DEA, Customs, and ATF translators are cleared only for access to law enforcement sensitive information and not national security information. In addition, raising the proficiency and clearance requirements for other law enforcement agencies would be costly and slow the acquisition of linguists to work on criminal investigations. Unless the overall pool of linguists is

¹ National Commission on Terrorism, "Countering the Changing Threat of International Terrorism" 2000; GAO report, "Foreign Languages: Human Capital Approach needed to Correct Staffing and Proficiency Shortfalls," 01/31/02.

significantly enhanced, shifting needed translation resources from one agency to another could also disrupt the operations of the agency losing the linguist support.

State and Local Law Enforcement Community

State and local law enforcement entities generally do not administer language proficiency tests, nor do they grant security clearances to their language specialists. For example, when the FBI's Chief of Language Services recently met with a senior official of a major metropolitan police department regarding the feasibility of such resource sharing, the official indicated that he did not want police officers to undergo polygraph examinations, thus precluding them from receiving Top Secret clearances.

The FBI could invest applicant processing personnel resources and funding on testing and clearing state and local law enforcement officers to the appropriate level. However, out of practicality, the FBI has generally chosen to invest those resources in creating a dedicated FBI language cadre.

Nevertheless, to ensure that any short, intermediate, or long-term benefits associated with the cross-agency sharing of linguists can be realized, the FBI pursued and received Executive Agent status for the National Virtual Translation Center (NVTC) initiative.

NVTC

The NVTC was established in response to Section 907 of the USA PATRIOT Act, which states "the Director of Central Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the appropriate committees of Congress a report on the establishment and maintenance within the Intelligence Community of an element for the purpose of providing timely and accurate translations of foreign intelligence for all elements of the Intelligence Community (IC)."

By memorandum dated February 11, 2003, the Director of Central Intelligence designated the FBI as the Executive Agent for the NVTC. The Language Services Section (LSS), Directorate of Intelligence (DI) has been charged with overseeing the administrative support to the NVTC; while the Director of Central Intelligence maintains oversight of NVTC operation. The NVTC's mission is to serve as a clearinghouse to facilitate timely and accurate translation of foreign intelligence for all elements of the IC. To accomplish this, the NVTC will work to:

- Provide a community portal for accessing language related tools and a broad range of foreign language materials in translated or vernacular form across security domains.
- Function within the Intelligence Community System for Information Sharing (ICSIS), which provides a common architecture and promotes interoperability and virtual access to databases across the IC.
- Support continued development and fielding of tools, web-based and other, designed to help process and exploit foreign language text and speech.
- Develop policies, procedures, and systems for managing NVTC translation requirements and translation services.

3. The needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

The increasingly global nature of the FBI's highest priority intelligence and law enforcement investigations continues to elevate its requirements for translation services. Since 9/11/2001, collection of information in certain critical languages (e.g., Arabic, Kurdish, Pashto, and Urdu) has increased by nearly 100% or more, while collection in other important languages (e.g., Chinese-Mandarin, Russian, and Korean) has increased at an annual average rate of 10 percent. The FBI is also experiencing greater and more consistent demands for languages such as Kurdish, Indonesian, and Somali. The FBI currently has sufficient translation capability to address promptly all translation needs with respect to high priority counterterrorism intelligence, often within 12 hours. There are instances, however, when translation needs cannot be addressed within 12 hours, or even within a week. For example, review may be delayed when the language or dialect involved is initially unidentifiable or when FBI translation resources are limited.

In order to address this escalating demand, the FBI executes a workforce planning model which links its recruitment and applicant processes to the threat environment. On the basis of this careful workforce planning, the FBI has been able to isolate and incrementally respond to its growing translation demands. Since 09/11/01, 778 Contract Linguists have been placed under contract (a net gain of 493) and 109 Language Specialists have been hired (a net gain of 34). As shown in the table above, since 9/11/2001, the FBI has increased its overall number of linguists by 67%, with the number of linguists in certain critical languages increasing by 200% or more.

While the FBI's successful recruitment and applicant processing system has recently made it possible to hire 250 to 300 new linguists per year, funding limitations inhibit the FBI's ability to further increase its translation capacity. The specific resource levels required to fully address all of the FBI's translation requirements are being finalized and will be included in the classified addendum to the President's FY 2006 Budget Request.

4. The status of any automated statistical reporting system, including implementation and future viability.

The only Department components that have automated statistical reporting systems for translation activities are the FBI and DEA. The FBI and DEA systems are described below.

FBI

The FBI's current statistical reporting system for digitally collected FISA data is Workflow Manager (WFM), which globally collects audio-FISA associated metadata from all FBI digital collection systems deployed in its field offices, and provides reporting on audio collection and review by language, case-file number, review status, etc. LSS has made substantial progress with the Investigative Technology Division (ITD) to resolve data errors, identify additional requirements, and make further improvements. WFM is now the primary, albeit not exclusive,

method of statistical reporting, in that it only captures audio FISA data.

A universal statistical reporting system will be made available with the deployment of the ELSUR Data Management System (EDMS), which will replace the current playback system on user desktops. EDMS will expand and improve on the FBI's statistical reporting capabilities in two ways: (1) it will capture statistics on all electronic FISA collections (voice and text), whereas WFM only reports statistics on voice collections; and (2) it will allow supervisors to generate real-time statistics using any combination of fields and drop-down menus, whereas WFM currently only produces canned reports. In the interim, LSS will work with ITD to develop a more flexible statistical reporting capability for WFM.

It should be noted, however, that the full migration of FBI FISA collection into EDMS is an ambitious undertaking both in terms of time and budget. The FBI is taking a phased approach by first deploying a tactical EDMS prototype which will be able to address the migration of data for priority counterterrorism cases by the third quarter of FY 2006. Achieving full migration of FISA data will require transitioning to a more robust strategic system starting in FY 2006 and continuing through FY 2009, and is dependent on necessary budget allocations in the intervening years.

DEA

DEA's Special Operations Division (SOD) Intercept Coordination Unit runs all Electronic Surveillance (ELSUR) requests from DEA's field offices. Data is cross-checked with systems of the Federal Bureau of Investigation (FBI), the Bureau of Alcohol and Firearms (ATF), Immigrations and Customs Service (ICE), U.S. Secret Service and the U.S. Postal Service. Many State and Local law enforcement agencies request ELSUR checks for any Federal records through DEA. In addition, DEA maintains a database that collects and reports to DOJ all wire intercept and pen register statistics.

5. The storage capabilities of the digital collection system or systems utilized.

The FBI and DEA are the only Department components that have specialized digital collection systems in connection with transaction activities.

FBI

With the upgrade of digital collection systems in 2004, the FBI's storage capacity at each site was significantly augmented. Current system configurations are designed to provide a minimum of thirty days on-line storage for all sessions on the system and to alert system administrators if the system is approaching a point at which deletion of sessions is required. The Investigative Technology Division continues to monitor the storage requirements of the field offices and will make system enhancements as required. All digital data is archived onto magneto-optical disks and can be retrieved based on searchable metadata.

DEA

With the upgrade of DEA's digital collection system, known as the *Translation/Transcription Support System* (T2S2), in FY 2005, storage capacity at each site will be significantly augmented. Current system configurations are designed to provide ample storage for all recorded sessions on the system and to alert system administrators if the system is approaching capacity. DEA's Office of Investigative Technology continues to monitor the storage requirements of DEA field offices and will make system enhancements as required. All digital data is archived onto magneto-optical disks which provides virtually limitless storage capacity, simply by adding additional disks.

6. **A description of the establishment and compliance with audio retention policies that satisfy the investigative and intelligence goals of the FBI.**

System controls in the FBI's digital collection systems are set to alert system administrators prior to any sessions being automatically deleted. If action is not taken prior to the system reaching critical levels, the system will begin an overwrite process to free up storage space, but only according to a preset protocol of deleting sessions based on their review status. This automatic deletion protocol is set to first delete sessions that have already been reviewed or processed, based on the review status of each session, in the following order:

1. Can Be Deleted
2. Reviewed
3. Tech Cut Produced
4. Forward Recv
5. Forwarded
6. Needs Further Review
7. Unreviewed

There is little chance of an unreviewed session being automatically deleted or overwritten. Even if that were to happen, cases and lines are set up by default for automatic archiving; all audio sessions are written to a magneto-optical disk immediately upon receipt.

To prevent critical audio from being removed from the on-line storage of the digital collection systems, LSS, in coordination with the FBI FISA Manager and ITD, implemented a prioritization schema in the August 2004 upgrade to digital collection systems field wide. This prioritization schema incorporates case tier and sub-tier designators based on the FBI's five-tier system. This prioritization will allow system administrators to protect sessions on high priority cases to prevent them from being overwritten. Again, even on the remote chance that an intercept is overwritten, all audio sessions are written to a magneto optical disk immediately upon receipt.

For the future system, EDMS will maintain copies of the original intercepts, not the evidentiary originals.² Furthermore, EDMS was never intended or designed for automatic

² The evidentiary originals are the magneto optical disks onto which the digital collection system writes the audio session immediately upon receipt.

deletion capabilities, as EDMS servers have a capacity for ten years worth of data. Manual procedures are available to delete information should that requirement exist for a specific reason, but EDMS does not give users or basic administrators the ability to delete data. EDMS also has backup capabilities to ensure that if data were deleted due to technical or human error, it could be retrieved.

7. A description of the implementation of quality control mechanisms for monitoring compliance with quality control procedures.

FBI

The FBI recognizes the vital importance of translation quality control procedures and practices. FBI linguists serve on the front lines of our intelligence collection and are responsible for reviewing, analyzing, and translating critical national security information. The FBI has maintained a four-pronged approach to translation quality control that includes (1) language proficiency testing, (2) personnel security, (3) professional development, and (4) quality assurance.

Language Proficiency Testing

First, to ensure each linguist has at least a professional level proficiency in English and the foreign language, all linguist applicants must pass a rigorous and comprehensive language test battery prior to hire. The FBI tests all language skills, i.e., speaking, reading, listening, writing, and translation, in accordance with standards developed by the Interagency Language Roundtable and adopted by the Office of Personnel Management.

Personnel Security

Next, each linguist candidate is subject to an exhaustive background investigation process, including a polygraph examination. Upon favorable adjudication, the candidate is granted a Top Secret security clearance. Each linguist is thereafter subject to the FBI's post adjudication risk management program that includes periodic security interviews, polygraph examinations, and information system audits.

Professional Development

Upon their entrance on duty, FBI linguists take a three-day course that delivers information on the FBI and Foreign Language Program's standards, evaluation programs, and quality assurance. Sophisticated equipment and computer systems used by linguists are demonstrated and special attention is paid to security and ethics.

In response to specific job skill requirements, linguists are thereafter eligible for specialized, language-specific training. This may include training in consecutive or simultaneous interpretation, or in advanced translation skills. The FBI also recently partnered with the National Security Agency's (NSA) National Cryptologic School for FBI linguists to attend one-day area

studies seminars and language enhancement training programs. These seminars are on various topics, and while some are offered in English, most are offered in a foreign language.

Quality Assurance

Prior to January 2003, responsibility for quality assurance reviews fell under the purview of the field office where the linguist was assigned. In January 2003, LSS instituted national Translation Quality Control Policy and Guidelines, which were later modified in December 2004. This was followed by the release of a Manual of Standards for Translation in December 2004.

The FBI does not yet possess the resource levels required for a dedicated linguist workforce to conduct and rate quality control reviews and must use the same linguists who are executing translation assignments in support of operational needs. In languages where demand for translation services exceeds translator supply, operational pressures often cause field supervisors to maximize productivity by foregoing strict adherence to quality assurance procedures. This situation was cited in the Office of Inspector General's (OIG's) report.³ The OIG also offered several recommendations for how our quality assurance procedures could be strengthened. For example, the OIG recommended that quality assurance reviews include not only material translated by linguists, but also materials deemed by the linguist to be not pertinent and never translated. We agree with these recommendations in principle and have incorporated the noted OIG recommendations into the modified quality control policy.

These quality control policy modifications provide specific instructions to all field offices, including clearly defined milestones for implementing measures that structurally improve our existing quality control program, as well as quarterly reporting mechanisms to monitor compliance. In addition, with increases made available in the Consolidated Appropriations Act, 2005, LSS will now be able to hire sufficient program management staff to guide and monitor field compliance.

Finally, LSS has coordinated with the Inspection Division to include a thorough review of a field office's Foreign Language Program (including compliance by the field with quality control policy) as part of the regular inspection schedule.

Operational Impact of the Quality Control Program

The FBI's Quality Control Program requires that after an initial week of training, all work performed by new linguists during their first 40 hours of service will be subject to review by a senior linguist. Work performed during the second 80 hours of service will also be heavily spot-checked and later checked with decreasing frequency as required. In all, it is estimated that each new linguist hired or contracted by the FBI will require an investment of at least 120 hours by a senior linguist dedicated to quality control.

In addition, the work of all FBI linguists will be subject to an annual review, thus requiring

³ U.S. Department of Justice, Office of the Inspector General, Audit Report 04-25, "The FBI's Foreign Language Program – Translation of Counterterrorism and Counterintelligence Foreign Language Program Materials," September 1, 2004.

an additional minimum investment of 20 hours per linguist-year. Therefore, current FBI linguist staffing levels (about 1300 linguists) will require approximately 26,000 senior-linguist hours (13 Full Time Equivalents (FTEs)) dedicated to annual reviews. In addition, an estimated 250 new linguists in a given year will require 30,000 senior linguist hours dedicated to initial training and quality control, plus another 5000 hours dedicated to the new linguists' first annual review.

The total requirement for addressing new linguists is approximately 17 to 18 FTEs. It is anticipated that this requirement will remain relatively constant once linguist supply meets operational demand, and that new hires will be counterbalanced by attrition. Similarly, annual reviews for existing linguists will require an additional 12 to 13 FTEs. Therefore, a successful quality control program would require a minimum investment of approximately 30 senior linguist work-years, as illustrated in the table below.

Operational Impact of the Quality Control Program					
Linguist Type	Task	# of Linguists	Hours per Linguist	Total Hours	FTE
New Linguists	Initial training and two weeks of work review	250	120	30,000	15
	First Annual Review	250	20	5000	2.5
Existing Linguists	Annual Review	1300	20	26,000	13
Total Estimate of FTE's to be Dedicated to Quality Control					30.5

While the FBI is not yet in a position to dedicate 30 senior linguists to quality control, given countervailing operational pressures, we expect to make substantial progress. We continue to aggressively recruit and process candidates with language proficiencies in those languages for which we have not achieved excess capacity. We also intend to take full advantage of program management workyears appropriated in Fiscal Year 2005 in order to centrally manage and monitor fieldwide compliance with our quality control policy, as well as the 43 Language Specialist positions which were also made available to strengthen our linguist cadre. For FY 2006, the Office of Management and Budget has requested an increase of 274 Language Specialist Positions and \$5,000,000 in Contract Linguist funding. If approved by Congress, this increase will provide the necessary relief and redundancy for a robust quality control program.

DEA

A vital tool in accomplishing DEA's mission is through consensual and court-ordered non-consensual communications intercepts, followed by real-time monitoring, translating and transcribing data and by translating documents and other media of potential evidentiary value. The purpose of communication intercepts and the collection of documents and other media are to further criminal investigations and to gather evidence for use by prosecutors during litigation. The knowledge gained is crucial to on-going investigations, and perfecting the procedures used is vital to the prosecution.

The many languages and cultural differences encountered during investigations, however, present tremendous barriers. As a result, the DEA has a continuous need for support of the agency's linguist program and has implemented translation service contracts at many of its field divisions.

For each contract, the Contracting Officer designates a Contracting Officer's Technical Representative (COTR) and delegates the issuance of task orders to a purchasing agent. The COTR is responsible for: receiving all deliverables; inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor that clarifies the contract effort, fills in details or otherwise serves to accomplish the contractual Statement of Work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment prior to forwarding the original invoice to the payment office and a conformed copy to the Contracting Officer. Consequently, the COTR is the individual who oversees the technical work of each contractor and monitors its quality. (The COTR, however, does not have the authority to alter/change contractual obligations, as that is the sole responsibility of the Contracting Officer.)

Quality control procedures

Prior to contract award, offerors are required to provide documentation to demonstrate their ability to meet the requirements found in each solicitation. Each factor (comprised of several sub-factors) is evaluated by a technical panel to ensure compliance with the requirements. The panel then determines which offerors should be considered for contract award.

Staffing. Firms must include a plan that demonstrates their ability to acquire the required amount of competent and qualified personnel to perform linguistic services. Firms must also describe their capability of furnishing qualified linguists in the primary language(s) as well as common and exotic languages as specified in each contract. Furthermore, firms must demonstrate their ability to provide proficient personnel for quality control review. Last, firms must demonstrate their capability to provide training of new and existing personnel to allow them to adequately perform the required services and to strive to improve performance.

Language Proficiency. Language proficiency testing in the source language(s) and English is required for all levels of linguists in the four basic communications skills (listening, reading, writing, and speaking). Testing must take place at a certified third party, such as interpreter associations and/or government entities. Evidence of language proficiency testing with acceptable results is required for all linguists prior to assignment to a DEA contract. The minimum acceptable language proficiency results are listed in each contract.

Security. Firms are required to submit a plan that details their security processes. It is essential that firms pre-screen personnel prior to submitting required security documentation to the DEA for processing of a clearance. Linguists are required to possess a DEA Sensitive clearance; individual linguists who do not meet the DEA's security requirements are not considered for employment under the contracts.

Employee Recruiting and Retention. Firms are required to provide a plan that describes their continuing recruiting and retention program as well as their procedures for determining and assuring the competency of personnel. This component is demonstrated by identifying the recruitment/hiring program and policies used to retain personnel to meet the Government's requirement. Information regarding the firms' methods for testing employees' abilities and ensuring that those abilities are maintained should also be outlined. If these requirements are not met, a high turnover rate may cause disruption in the wire room.

Past Performance. During the pre-award stage, firms are evaluated on their performance under existing and prior contracts for same or similar services. During the life of the contract, firms are evaluated in four areas: quality of product or service; cost control; timeliness of performance; and business relations. Individual linguists are not evaluated or considered with the exception of Key Personnel.

Contract Administration. In order to ensure that any problems are quickly identified and rectified, contract administration includes frequent communication between the contractor's contract administration staff and the DEA's Contracting Officer and Contract Specialist. In addition, timely submittal of all required reports and other contract deliverables are monitored. Further, timely processing of any required modifications (to either the basic contract or any task order) or other documentation is considered.

Financial Management. Financial management includes the review of reports and invoices for reconciliation of work ordered and actually performed, and the review of actual expenses. This review is essential because of the reconciling process, which consists of reconciling obligations versus expenditures to monitor Undelivered Orders (UDOs) as well as to monitor preparation, submittal and approval of invoices to avoid performance issues that might arise due to finances.

Mechanisms to monitor compliance

The Contractor is required to produce and deliver a monthly administrative report appropriate for monitoring work performance. The Government requires the report monthly even if task orders are not active. The Government requests that the contractor submit this administrative report with its monthly invoices. The report must include a financial statement; personnel status; security packages information; and a brief description of any technical or administrative problems that have occurred during the reporting period under any task order issued, including any problems that are expected to occur during the next reporting period.

In addition, DEA encourages performance evaluation meetings between the COTR and the contractor in order to resolve any problems that arise during the performance of the contract.

EOIR

In a manner similar to DEA, EOIR also uses the contract award and management process as a means of controlling the quality of the performance of the contract linguists that it uses in its Court Interpreter program. This includes structured screening and performance interviews, a

bi-directional interpretation test that specifically verifies an interpreter's ability in English and the foreign language, a comprehensive interpreter orientation, a court specific training program, evaluation of the first hearing tape, on-going evaluations both on site and reviews of hearing tapes and written reviews by immigration judges.

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary
Sunset Provisions of the USA Patriot Act

April 5, 2005

Good morning Mr. Chairman, Senator Leahy and Members of the Committee. I am pleased to be here today with the Attorney General to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its efforts in the war on terror. For almost three and a half years, the USA Patriot Act has changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act. As you know, several of these provisions are scheduled to "sunset" at the end of this year. I firmly believe that it is crucial to our national security to renew these provisions. Without them, the FBI might well be forced into pre-September 11th practices, requiring us - agents, analysts and our partners - to fight the war on terror with one hand tied behind our backs.

USA Patriot Act SUNSET PROVISIONS

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing).

Section 201 brought the federal wiretap statute into the 21st century. Prior to its passage, law enforcement was not authorized to conduct electronic surveillance when investigating crimes committed by terrorists, such as chemical weapons offenses, killing U.S. nationals abroad, using weapons of mass destruction, and providing material support to terrorist organizations. Section 201 closed an existing gap in the Title III statute. Now Agents are able to gather information when looking into the full range of terrorism related crimes.

Similarly, Section 202 brought the criminal code up to date with modern technology by adding felony offenses under the Computer Fraud and Abuse Act, such as computer espionage, extortion and intentionally damaging a federal government computer, to the list of wiretap predicates in 18 U.S.C. §2516(1). This provision eliminated an anomaly in the law and now permits Agents to obtain wiretap orders to monitor wire and oral communications to investigate serious computer crimes.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. If Section 203(b) were allowed to expire, FBI Agents would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, but would arguably not be allowed to share that same information with the CIA. This result would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government. Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials.

The information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the USA Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the USA Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the USA Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. Clarification of information sharing abilities, due in part to Section 203, eliminated that hesitation and allows agents to more openly work with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, our Field Offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships. Even Legal Attaches (Legats) notice improved relationships with intelligence agencies. If even a portion of the information sharing capabilities is allowed to 'sunset' or terminate, then the element of uncertainty could be re-introduced and agents will again hesitate and take the time necessary to seek clarification of complicated information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's

ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI must initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeiting goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as the Intelligence Community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity. In one such case, information from a criminal Title III and criminal investigation was passed to Counterterrorism, as well as intelligence community partners, because the subject of the criminal case had previously been targeted by other agencies. Information sharing permitted each agency to pool their information and resources to investigate the interplay of criminal and foreign intelligence activity.

In one instance, a terrorism case initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantities of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The operation resulted in the arrest, indictment and subsequent deportation of the subjects, Syed Mustajab Shah, Muhammed Afridi, and Iiyas Ali, from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda.

Criminal enterprises are also frequently involved in, allied with or otherwise rely on smuggling operations. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has identified smugglers who provide false travel documents to special interest aliens, deal with corrupt foreign officials, and financially support extremist organizations, as well as illegitimate and quasi-legitimate business operators in the United States, who not only use the services of illegal aliens, but are also actively involved in smuggling as well.

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen as a leader among a group of Islamic extremists residing in the U.S. The

subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case.

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

Section 204 is essentially a technical amendment. It clarifies that the law which governs the installation and use of pen registers and trap and trace devices will not interfere with certain foreign intelligence activities that fall outside the definition of "electronic surveillance" in the FISA statute. The provision also clarifies that the exclusivity provisions in Title 18 section 2511(2)(f) apply not only to the interception of wire and oral communications, but also to the interception of electronic communications.

Section 206 - Roving FISA Surveillance

With this provision, when a FISA target's actions have the effect of thwarting surveillance, such as by rapidly switching cell phones or even meeting venues, the Court can issue an order directing an as yet unknown cell phone carrier or other company to effect the authorized electronic surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order.

Section 206 has been extremely helpful especially with regard to international terrorism and foreign counterintelligence investigations where targets move quickly and often act evasively to avoid detection. Field Offices have observed counterintelligence targets change services for hard-line telephones and cell phones numerous times. The roving authority allows us to continuously monitor these targets without interruption. By minimizing the need to return to the court for additional authorizations, it also has allowed agents to more expeditiously conclude investigations.

In one case, a roving FISA on a subject's cellular telephone was approved for the subject of a counterintelligence investigation who, per the usage of tradecraft, is directed to change his cellular phone at regular intervals. The roving FISA allows us to continue coverage on all cell phones the subject obtains.

Section 207 - Extended Duration for Certain FISAs

Section 207 extends the standard duration for several categories of FISA orders. Before the enactment of the USA Patriot Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of ninety days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than 45 days, unless the target was a foreign power, in which case, the order could be issued for one year. This provision allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for ninety days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance may apply or extend for periods of 120 days, and renewal orders can be extended for up to one year.

Section 207 has led to reduced paperwork in certain categories of cases. In addition, it has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed agents to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail.

Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation.

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

Service providers have voluntarily provided information under this provision. Such disclosures often included both e-mail content and associated records. This provision has also been utilized to quickly locate kidnaping victims, protect children in child exploitation cases, and to quickly respond to bomb and death threats. Legats have also utilized this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing death or serious injury.

In one instance, an FBI Field Division received a bomb threat after hours. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, the FBI JTTF Agents began working with various communications providers to locate the caller. The caller was identified as a result of an emergency disclosure pursuant to this provision. An interview of the subject was conducted and the threat was determined to be non-credible by 11:00 a.m.

In a kidnaping case, a 14-year-old girl was abducted. As a result of the FBI's use of this provision, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours. This is but one example of how essential this provision is for child abduction cases.

Section 214 - FISA Pen/Trap Authority

The FBI may now obtain a FISA pen/trap and trace order from the court if "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation 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." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications, comparable to the criminal pen/trap provision.

The results from these pen/trap orders often help agents to determine links between the subjects of different terrorism investigations, identify other unknown associates of the subject, discover contacts for potential assets, and develop the subject's personal profile. When pen/trap orders are quickly obtained, they allow agents to more quickly identify the associates tied to the subject of international terrorism investigations than if the agents were required to wait for service providers to respond to subpoenas for toll records, which can take several months. The old standard required more fact gathering to meet the threshold to obtain the pen/trap order, making this technique less effective and sometimes even preventing the use of this technique altogether if the window of opportunity was missed. The FISA pen/trap orders that have been obtained have been used on both terrorism and counterintelligence cases.

In one terrorism case, the only phone that the Field Office could prove was used by the subject was his associate's phone. Additionally, the Field Office had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the office may not have succeeded in obtaining the FISA pen/trap order. The standard

established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations.

In another example, use of this section allowed FISA pen/trap authority based on the fact that information was likely to result in foreign intelligence information. This provision allowed the Field Office to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject, the organization and terrorism-related matters.

Section 215 - Access to Business Records under FISA

Section 215 changed the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records (i.e. hotels, motels, car and truck rentals) to include "any tangible things (including books, records, papers, documents, and other items) for an investigation 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."

Obtaining business records is a longstanding law enforcement tool. Ordinary grand juries for years have issued subpoenas to all manner of businesses for records relevant to criminal investigations. Section 215 authorized the FISA Court to issue similar orders in national security investigations. It contains a number of safeguards that protect civil liberties. Section 215 requires FBI Agents to get a court order. Agents cannot use this authority unilaterally to compel any entity to turn over its records. In addition Section 215 has a narrow scope. It can only be used to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. It cannot be used to investigate ordinary crimes, or even domestic terrorism.

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The USA Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

Under this provision, the FBI was able to monitor the communications of an international

group of "carders" (individuals that use and trade stolen credit card information). The group utilized a variety of methods to conceal their identities. The owner of the hacked computer was not aware of the misuse, and considered all individuals misusing its computers to be trespassers. The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of 2003. Without the ability to monitor these communications, it would have been unlikely that the FBI could have identified the trespassers.

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 amended FISA to require a certification to the FISA Court that obtaining foreign intelligence gathering is "a significant purpose" of the FISA surveillance or search, rather than a "primary purpose" of such surveillance. Section 504 amended FISA to clarify that personnel involved in a foreign intelligence investigation can consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were intended to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their investigations at risk.

As stated above, FBI Field Offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision makes it clear that prosecutors can be involved in the earliest phases of an international terrorism investigation. AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

The ability to have criminal prosecutors involved in the earliest investigative phases of terrorism cases allows counterterrorism investigators to utilize the full selection of both intelligence and criminal investigative tools, enabling them to select and interchange these tools to meet the investigative demands of each particular case. Field Offices use criminal prosecution, or the threat thereof, in furtherance of the intelligence objective to disrupt and dismantle terrorism, towards the ultimate goal of preventing terrorist acts. One Field Office notes that if 218 were allowed to "sunset," its aggressive and effective investigative approach toward terrorism would be "severely crippled."

Section 220 - Search Warrants for Electronic Evidence

Section 220 of the USA Patriot Act enabled courts with jurisdiction over an investigation to issue a search warrant to compel the production of information held by a service provider located outside the district, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

The FBI routinely relies upon this provision when a search warrant is used to obtain the content of e-mail messages and other related information from Internet service providers (ISPs) in accordance with 18 U.S.C. § 2703.

Prior to the USA Patriot Act, if an investigator sought a search warrant to obtain the content of unopened e-mail from a service provider, the investigator was required to obtain this search warrant from a court in the jurisdiction where the service provider was located. To accomplish this, the case agent would brief an agent and prosecutor located in the ISP's jurisdiction on the facts of the case so that they might appear before the court and obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest ISPs are located in a few districts such as, the Northern District of California and the Eastern District of Virginia, these offices were faced with a substantial workload just to obtain search warrants for other offices.

While the USA Patriot Act maintained the legal standard of probable cause that must be met before the search warrant could be issued, it eliminated the additional bureaucratic paperwork necessary to obtain that warrant in a different jurisdiction than the investigation itself. This eliminated the need to involve additional agents and prosecutors located in the same jurisdiction as the ISP. Therefore, this provision expedites the process and minimizes the labor involved without altering the privacy protection afforded the e-mail and other associated records.

Field Offices repeatedly stated that this was very beneficial to quickly obtain information required in their investigations. The information obtained from these search warrants often leads to additional electronic evidence that is otherwise easily and quickly lost. Minimizing the time required to obtain the initial information from the ISPs is a significant asset to the investigations.

In the "Virginia Jihad" case, six subjects pled guilty and three were convicted of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. They received sentences ranging from a prison term of four years to life imprisonment. As a part of this case, court orders were issued to Internet Service Providers throughout the country to obtain information that resulted in valuable intelligence and criminal evidence used in the successful prosecution. Due to Section 220, all the court orders were issued by the district court where the prosecution occurred making the process much faster and more efficient.

This provision is regularly used in child pornography cases as agents obtain information from ISPs regarding those trading sexually exploitive images of children. This expedites the investigative process and minimizes the number of FBI, U.S. Attorney, and judicial personnel involved in the process, freeing them to more aggressively pursue investigative matters.

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the USA Patriot Act, individuals were permitted only in limited

circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation by creating an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISA Court to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent of a foreign power, such as an international terrorist or spy. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies, to carry out such court orders. Prior to the passage of the USA Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISA Court under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay.

In an FBI Field Office, a case agent was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target was an espionage subject.

Section 213 - Delayed Notice Search Warrants

While not scheduled to sunset, the USA Patriot Act's delayed notice provision, Section 213, has been the subject of criticism and various legislative proposals. The FBI believes that Section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. It is important to note that delayed notice warrants were not created by the USA Patriot Act. Rather, 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 USA Patriot Act ensures 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 had been executed.

Delayed notice search warrants provide a crucial option to law enforcement and can only be issued if a federal judge finds that one of five tailored circumstances exists. The FBI has requested this authority in several cases. In most instances, the FBI seeks delayed notice when contemporaneous notice would reasonably be expected to cause serious jeopardy to an ongoing investigation.

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the USA Patriot Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address another area in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

Administrative Subpoenas

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and enforcement is difficult. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously, Section 215, which does not contain an emergency provision, may not be the most effective process to undertake. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal should provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

CONTINUED OVERSIGHT OF THE USA PATRIOT ACT

TUESDAY, MAY 10, 2005

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:30 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Arlen Specter, Chairman of the Committee, presiding.

Present: Senators Specter, Kyl, Cornyn, Leahy, Biden, Feinstein, Feingold, and Durbin.

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

Chairman SPECTER. Good morning, ladies and gentlemen. It is precisely 9:30, so the Committee on the Judiciary will now proceed to a hearing on the PATRIOT Act.

This is our third hearing. Earlier we had testimony from Attorney General Gonzales and FBI Director Mueller and then we had a closed session in examining the provisions of the PATRIOT Act. As we have stated, we are going to be looking at specific factual situations to make our determinations as to what changes there ought to be in the PATRIOT Act, and I do not say "what changes, if any," because Attorney General Gonzales has stated his own view of the need for some changes. I think his changes are probably not as extensive as will be recommended by the Committee, at least in legislation. But I compliment the Attorney General for his openness in meeting with quite a number of groups which have objections to the PATRIOT Act. And I believe that that is a very salutary approach to give people an opportunity to be heard. Sometimes you find out things you had not expected. Sometimes you even change your mind if you have that kind of a hearing—a listening as well as a hearing. And it certainly is helpful on the overall approach to the issue if all sides feel that they have at least been heard and had a chance to present their views.

We are going to be looking this morning at a continuation of the delayed notice on the search warrants. We have had some specification from the Department of Justice on the specific cases, their representation that there have been some 28 occasions where the delayed notice was necessary to avoid seriously jeopardizing an investigation. We are going to make a review of those situations and our own factual determination.

We are concerned about the provision on business records as to whether there ought to be a showing of probable cause or at least

(315)

some showing beyond that which is now in the statute. And there has been some substantial concern and worry over the provision for library records and medical records. And we have been advised that the Department of Justice has never used them for library records, and that raises the obvious point: If it hasn't been used in that line, wouldn't it be wise to have a specific exclusion unless there can be a showing by the Department of Justice of the necessity for it?

There are provisions which we will be taking a look at on the separation of the wall. I think that is a generalization. It is desirable to have the separation of the wall on foreign intelligence and criminal matters if evidence is uncovered in a Foreign Intelligence Surveillance Act case and it shows criminality, to be able to proceed there. But there has to be a good-faith effort by the individuals applying for the warrants to make sure that they are on the right line.

We have a long list of witnesses today. The lead witnesses are two of our colleagues: Senator Craig and Senator Durbin. The time limits will be set at 5 minutes, which is our Committee's custom, and I am now going to yield to my distinguished Ranking Member. And I want the record to show that I am yielding back a minute and 10 seconds.

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

Senator LEAHY. Mr. Chairman, I caught the hint.

I am delighted to be here. I want to compliment the Chairman for doing this, and I appreciate his leadership in oversight. This Committee, as much as any committee in the Senate, should be involved with serious oversight of serious matters, and under his chairmanship, I am glad to see us going back to that tradition. And I appreciate it. All of us, whether Republicans or Democrats, are better off, and ultimately not only is the Senate better off with real oversight, but the American people are better off. And even though sometimes Presidents—and I have heard complaints from Presidents of both parties—complain about oversight, they are usually better off if we do it.

It is interesting to note that this is catching. Our counterparts in the other body are also holding another hearing this morning on the PATRIOT Act. The Chairman said the Senate Select Committee on Intelligence has heard it. It has been the focus of more than a dozen hearings this year alone.

It is no mystery why, when we seem to have a difficult time to get oversight hearings in other areas, important areas, we are getting it here.

Just a little history. I will tell you a story about the history of this. In the final negotiating session of the law, former House Majority Leader Dick Armey, a man not normally seen as my political soul mate, he and I worked together and we insisted on adding sunset provisions for certain governmental powers that have great potential to affect the civil liberties of the American people. And these sunset provisions are the reason we are here today. It is why we are revisiting the PATRIOT Act. We have to revisit it because of what Leader Armey and I put into the Act.

It also explains why we are getting some answers from the Department of Justice, answers that we were denied for years, but under the persistence of Chairman Specter and the tolling of the sunset provisions, suddenly the answers are coming forth.

Now, the PATRIOT Act is not a perfect piece of legislation. I have been here 31 years. I have a hard time picking out what has been a perfect piece of legislation. I said as much when we passed it just 6 weeks after the 9/11 attacks, and I was Chairman of the Committee at that time.

In negotiations with the administration, I did my best to strike a reasonable balance between the urgent need to address the threat of terrorism and the need to protect our constitutional freedoms. I was able to add many checks and balances that were absent from the administration's draft along with provisions to address other concerns such as border security and the terrible problem the FBI had with the lack of translators. Other members of the Committee and in Congress were able to include improvements as well. But I made sure that we would have oversight. I always knew and noted at the time that we in Congress would have to revisit these issues when the immediate crisis and the emotional aftermath of the crisis had abated.

Now, we had some, even one on this Committee, who wanted to pass this legislation without even reading it, before it even came up from the administration. Fortunately, cooler heads prevailed. Cooler heads won over that sense of panic, and we actually read the legislation before we passed it.

Now, legitimate concerns have been raised about various powers granted by the PATRIOT Act not so much for how they have been used but for how they could be used—not so much how they are used but how they could be used—and for the cloak of secrecy under which they operate. Since September 11th, Americans have been asked to accept restrictions on their liberties. They deserve to know what they are getting in return. Until then, this Senator is not going to ask the American people to give up any more of their liberties unless they know exactly what they are getting in return.

So the sunset provisions ensured that. Dick Arney and I were afraid that the administration would not tell the American people what was going on. We were right. Now the answers are coming. And, Mr. Chairman, I am delighted we are here at this point, and I am glad these sunset provisions are there because finally we will get some answers.

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

I have 31 seconds left.

[Laughter.]

Chairman SPECTER. Thank you very much, Senator Leahy, for that erudite statement and even more for the 31 seconds.

Our first witness is our distinguished colleague, Senator Larry Craig, who served in the House of Representatives before coming to the United States Senate in 1990. He had been a member of this Committee in the 108th Congress, and we know that his departure was occasioned by a difficult matter of Committee selection. But we definitely miss him here.

He is the principal author of the so-called SAFE Act, the Security and Freedom Enhancement Act of 2005. And Senator Craig and others who are sponsors of that Act have been cited as evidencing a concern about the provisions of the Act as to whether they are all necessary after 9/11 where, as Senator Leahy has accurately said, we passed the legislation and whether modifications ought to be made. And his sponsorship of that Act has really drawn into sharp focus the fact that people on all phases of the political spectrum—the left, the right, the center—have all expressed concerns, which is a signal for very close attention on the legislative process. So thank you for joining us, Senator Craig, and the floor is yours.

**STATEMENT OF HON. LARRY E. CRAIG, A U.S. SENATOR FROM
THE STATE OF IDAHO**

Senator CRAIG. Well, Mr. Chairman, first and foremost, thank you for holding this hearing on the USA PATRIOT Act. As Senator Leahy mentioned, the House has held hearings; Intel has held hearings. Last year, as you referenced, when I served on this Committee, we held some hearings. But it is most appropriate for this Committee to once again review the PATRIOT Act and to make sure that changes, I think, that will be made in it are appropriate and necessary.

When we originally passed PATRIOT, Congress did a number of good things. We came together in a bipartisan fashion to carry out a number of responsibilities of the Federal Government had to do one thing, and that was to protect our citizens. And we did something else that was very wise. We anticipated, as Senator Leahy mentioned, that hindsight would give us a better perspective on dealing with terrorism, and we put sunsets in the PATRIOT Act to force a re-examination at a later date of the expanded powers that Congress has given the Federal Government.

Since then, we have looked at how the law is working and what impact it has had. The 9/11 Commission has given us some additional insight. Notably, that Commission cautioned us that the burden of proof is on Government to justify keeping expanded PATRIOT powers. This caution should be at the forefront of this Committee's deliberations now that the day has come to decide what to do with the expiring provisions of the PATRIOT Act.

But I would also submit that even if the Government justifies its use of expanded powers, this Committee should ask a second question: How can we prevent the future abuse of these powers? This is the key question, I think, Mr. Chairman, a question that has certainly haunted me ever since I saw lives lost in my State of Idaho at the hands of people who were unquestionably well-intended in trying to preserve the peace. The folks back home find it awfully hard to just sit back and trust Government to do the right thing without the adequate checks and balances to prevent harm in case something goes wrong, in the case that good people make mistakes or have to turn over their cases to not-so-good people. And, of course, Mr. Chairman, you know what I am talking about. You held hearings on that situation in Idaho a good number of years ago where good people did bad things, and as a result of those hearings, we made changes in the way our Federal Government and the way the FBI operated.

Our Nation has a great tradition of balance in the enforcement of its laws. PATRIOT should rest squarely in that tradition. Let me tell you of an experience I had this last week about tradition. I was at the police academy camps just outside of Amman, Jordan, where we are training thousands of Iraqis to become policemen. And one of the principal pieces we put in their new mental make-up as a law enforcement officer is how to Act in a democratic way. They do not understand the democratic principle of law enforcement and that those who are arrested have rights and should be treated forthrightly. I thought that most fascinating, that that is the one thing we are attempting to instill in law enforcement officers, and here we are reviewing a most important law in which we must understand that the greatest threat is life and liberty of our citizens at the hands of our Government if our Government goes wrong.

I am not here to stand up for the bad guys. I am worried about what happens when good guys make mistakes in some future administration and when the weakest links among us decide to abuse the law for their own ends, such as stifling political disagreement.

The point is that our law cannot be written for the best and the brightest. They must also anticipate enforcement by the worst and the weakest. That was certainly the skeptical approach taken by our Founding Fathers, Mr. Chairman, when they crafted the blueprint of our Federal Government, the Constitution, and placed strict limits on the enormous powers of Government.

I ask you to keep in mind these very thoughts as you review PATRIOT Act. If we cannot change human nature and prevent all abuses, the very least we can do is prevent the harm that might follow from them. This is where our bill comes in. You are right; it is a bipartisan bill. Senator Durbin will testify later. He and I and Senator Feingold and many of our colleagues have introduced S. 737, the Security and Freedom Enhancement Act that you referenced a few moments ago. This bill would make several narrow, targeted changes in PATRIOT. S. 737 is by no means the final word on amending PATRIOT. It addresses only a few of the more controversial PATRIOT provisions.

I am well aware there are colleagues who are advocating additional changes in the law or the different approaches in the sections of the law as we have targeted in the SAFE Act. I want you to know there are some changes from last year's rendition of the SAFE Act. We have taken a couple of those changes because the Department of Justice suggested that changes ought to be made, and we have incorporated that potential intimidation of witnesses should be another justification for allowing delayed notice of search. We have also responded to the concern that it is too burdensome to require weekly renewal of the authority of delayed notice of search.

I notice my time is up. I will submit the balance of my statement to the record, Mr. Chairman, but once again, this is as much about the future of the law and its enforcement as it is about current-day law and, once again, making sure that those firewalls are in place to protect the liberty and the freedom of our citizens.

So I hope you will take this into consideration. We think we have put together a very strong, bipartisan approach to targeted amend-

ments. We are not here to speak of repeal. We are here to speak of strengthening and clarifying PATRIOT Act.

Chairman SPECTER. Thank you very much, Senator Craig. You are accorded a little more leeway when you are not a member of this Committee. Committee members have to stop exactly on time. But since you are not a member of the Committee—

Senator CRAIG. Well, Mr. Chairman, I had the privilege of serving on this Committee before, and I remember that there were not the time rules there are today. I wish I were serving here today.

[Laughter.]

Chairman SPECTER. Thank you.

Does anybody have any questions for Senator Craig?

Senator LEAHY. Yes. Senator Craig, one, I appreciate your testimony. We talk about Ruby Ridge. As you know, as the Chairman I lived that for weeks and weeks and weeks with the hearings we had. And I agree with your thought that good people did bad mistakes on both sides.

I think the tragedy of that one was—I remember the last question I asked Mr. Weaver or the last series of questions. I asked him if he thought he had been treated fairly in the hearings. He said he had. I asked him whether he had a different view of his Government, having seen the hearing that Senator Specter and I and others had held. He said a much different view. And I said knowing now that the questions could be asked, fairness could be brought forward, what would you have done in retrospect? And I remember the very sad answer: "I would have come down from the mountain."

And I think you and I would probably be in agreement in 99 percent of the areas—or 100 percent of the areas where things went wrong. And that is what we want to avoid, that things get out of control, that we do not have the oversight.

I think you would agree with me, would you not, that there are a lot of very, very good parts in the PATRIOT Act? I can think of meaningful judicial review of surveillance authorities where the judge is a real fact finder, not just a rubber stamp; meaningful oversight, timely reporting. These are things that we should try to retain. Would you agree?

Senator CRAIG. Well, I would agree, and I also believe that in this new world we live in of terrorism, where preemption is so important because it saves lives prior to an act. You know, we were in the mode of going out after an Act occurred and finding all of the possible findings made and trying to create or craft a circumstance behind a guilty party, that is too late in this new business we are into. So there has to be some way of preemptive action while safeguarding the right of our citizens. And I think that our amendments and the Act itself is the right combination.

Senator LEAHY. Would you agree with me that a touchstone we should have—Benjamin Franklin said, and I paraphrase—I was not there, but I paraphrase. He said something to this effect when writing the Constitution and Bill of rights. He said a people who would give up their liberties for security deserve neither.

Senator CRAIG. Well, I certainly don't disagree with that, and I think that that is a very important test for all of us. That is something that very early on in this new world we are living in, we had

to figure out how much we were willing to give up and how we gave it up.

I am still extremely frustrated every time I walk through an airport and I find some person going through my suitcase. That is an invasion in my privacy. I have given it up in the name of safe flight. How much more do our citizens have to give up on a daily basis? I find it very difficult to believe that the Federal Government can enter my home, strip my hard drive off my laptop, go through my records, walk out the back door, leave it neat and clean as if unentered, and never tell me they were there. That is a step too far. And that is a step too far in every circumstance, unless there is reasonable and just cause and it has been demonstrated to a judge. We are not even taking the right of entry away in the first instance. We are simply establishing reasonable notification after the fact.

Senator LEAHY. I would hope that both liberals and conservatives would agree on what you have just said. Somebody once said to me, you know, probably the proudest thing you have in your life is being a United States Senator. I said, no, the proudest thing is being an American. And that I did not have to work for. I was born in the State of Vermont, born that way. My grandparents immigrated to this country to become—not even speaking the language, but to become Americans, and it is because of the freedoms we have. I think if there is an area where we can make common cause, all of us, it is in protecting those freedoms. And we could protect them and have a secure Nation. Of course, we face different threats today. Of course we do. But if this great Nation cannot defend our security and protect our liberties at the same time, what do we have?

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Leahy. Senator Cornyn?

**STATEMENT OF HON. JOHN CORNYN, A U.S. SENATOR FROM
THE STATE OF TEXAS**

Senator CORNYN. Thank you, Mr. Chairman.

Mr. Chairman, I do appreciate your holding these oversight hearings on the PATRIOT Act, and I think it is very important for all the reasons stated. And I appreciate our good colleague and friend Senator Craig for expressing the concerns that he has. While I have some reservations about his proposed solution, I agree wholeheartedly with his concerns. And I think it is important that we proceed to try to determine what the facts are.

Unfortunately, as far as the PATRIOT Act is concerned, people condemn the PATRIOT Act entirely based on not the facts but on emotion and on spin. I think Senator Feinstein has been the one who I have appreciated her efforts to ascertain the facts during the course of our oversight hearings on the PATRIOT Act by determining whether there is any substance to some of the complaints. And, in fact, there is, I have concluded, very little substance.

While we all are left to speculate about the effect of laws that we actually pass, the best teacher is experience. And I think we have seen the PATRIOT Act has held up well in experience in terms of providing security but not unduly jeopardizing our liberty.

So I appreciate your having these hearings. I look forward to the testimony. But I hope that in the end we will do as we always try to do, but sometimes don't succeed, and that is to make our decisions based on the facts and on experience rather than on emotion.

Thank you very much.

Chairman SPECTER. Thank you very much, Senator Cornyn.

Senator Feinstein, if it is acceptable to you, may we turn to Senator Durbin, who has just arrived?

Senator FEINSTEIN. Absolutely.

Chairman SPECTER. He is our second witness. I know when your round of questioning comes, you will want to have some questions for Senator Durbin.

Senator FEINSTEIN. Thank you.

Chairman SPECTER. We welcome you here, Senator Durbin, elected to the United States Senate in 1996 and re-elected in 2002, a distinguished record on many, many very important substantive matters, was elected as assistant Democratic leader, which he serves on at the present time. We thank you for joining us, and I don't have to comment to you, Senator Durbin, since you are a member of this Committee, about the time limitations.

**STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR
FROM THE STATE OF ILLINOIS**

Senator DURBIN. Mr. Chairman, thank you very much, and my apologies to you and the members of the Committee and to my colleague, Senator Craig, for my tardiness here. Unfortunately, as you mentioned, some of the leadership responsibilities conflict with this hearing schedule.

Thank you for holding this meeting, Mr. Chairman. I commend you for doing it. I think it is a timely thing to do. There isn't one of us in this room who does not recall exactly where we were when 9/11 took place and we learned about that terrible tragedy. And there is hardly a one of us who does not believe that that was one of the most traumatic moments in our lives when it comes to the history of our country, that we were the victims of this invasion, killing 3,000 innocent Americans. It led us to take extraordinary action on Capitol Hill as well as across the Nation to protect ourselves. And one of the most extraordinary things we did was the passage of the PATRIOT Act.

I felt at the time it was the right thing to do. I was not 100 percent certain because I knew that my decision on this bill was somehow caught up in the emotion of the moment, the concern of the moment about whether or not another attack was on the way, how we would save innocent lives from the horrors of what happened in Washington and in New York. And, luckily, I think wisdom prevailed in that we included in that PATRIOT Act sunset provisions saying that our actions at that time would not be permanent law, that we would come back and revisit them to decide whether they were still wise decisions at a later time. Your hearing sets the stage for that conversation, an important national dialogue.

First, I think we need to try to establish some fundamental principles. The American people want Congress to strike a balance, to protect civil liberties but give the Government the power it needs to fight the war on terrorism. There are many communities in

States across the Nation who have serious concerns about whether the PATRIOT Act struck that balance. I ask unanimous consent to enter into the record a list of the communities which have passed resolutions expressing concern about the PATRIOT Act.

Chairman SPECTER. Without objection, they will be made a part of the record.

Senator DURBIN. Thank you.

Second, as the independent bipartisan 9/11 Commission concluded, when the Government seeks to expand its power—and I think this is crucial. Senator Craig and I have thought about this and really make this kind of the linchpin of where we are coming from. When the Government seeks to expand its power, the burden of proof should be on the Government to demonstrate that that power is needed to combat terrorism. This means the Justice Department must provide Congress with information to assess how the PATRIOT Act is being used.

You were kind enough to have a meeting in 407, a closed-door meeting with some classified information about the use of the PATRIOT Act. It is unfortunate that we cannot share with the colleagues in this Committee as well as members of the public exactly what was said at that time. Some of the things would be said in defense of the PATRIOT Act, some maybe used in criticism of it. But that information is not forthcoming, so it is very difficult for us to make an honest, open, and objective assessment for the American people to be the final arbiter as to what is fair in terms of the future of the PATRIOT Act.

Third, it is our constitutional duty as Senators to examine closely legislative proposals that expand Government power such as the PATRIOT Act. We should ensure that they are needed to fight terrorism, that they include adequate checks and balances, and they will not lead to civil liberties violations.

I also ask unanimous consent at this time, Mr. Chairman, to enter into the record the statement of principles of the new caucus that Senator Craig and I have founded, the Bill of Rights Caucus.

Chairman SPECTER. Without objection, it will be made part of the record.

Senator DURBIN. Several of our colleagues, including Senator Feingold from this Committee, have joined us in introducing the SAFE Act. It is narrowly tailored. It is a bipartisan bill.

Mr. Chairman, if you came to the press conference where we announced the SAFE Act, you would have seen the most unusual gathering of political groups I have ever seen at any announcement: from the left, the American Civil Liberties Union; from the right, the American Conservative Union. Groups that were good-government groups, groups that, frankly, never come together came together behind the SAFE Act. It shows that if Senator Craig and I can sit at the table in agreement that there is some fundamental principle at stake here, and that principle is to protect our rights and liberties. We believe on the right and on the left that we should come together as we have sworn to uphold this Constitution.

We do not want to end the PATRIOT Act. We want to amend the PATRIOT Act. We think reasonable changes in the PATRIOT Act

will protect individual rights and liberties and also give the Government the tools it needs to make America safe.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Durbin.

Senator Feinstein?

Senator FEINSTEIN. Thanks very much, Mr. Chairman, and I want to thank my two colleagues. I think it is very interesting to hear your point of view.

I have been, as I have said before, puzzled because initially I think there was a great deal of misunderstanding about the PATRIOT Act, and confusion. I think a lot of the comments were directed toward PATRIOT II, which never came to the Hill, and also to immigration law, referred to as the NSEERS law.

To this day, I know of no abuse of the PATRIOT Act in virtually any given section. Can either of you provide an abuse of the PATRIOT Act?

Senator CRAIG. Senator, I agree with your statement, and if you will remember my comments of a few moments ago, this is all about the future and making sure we put in place those safeguards that will never tolerate or allow abuse. But I cannot disagree with you. In my experience on this Committee and the hearings that I have attended, I have listened very closely because I am a critic in a limited and targeted way. I do not believe it has been misused to date, to my knowledge. But I do believe there are potentials built within it for misuse, and that is what we address.

Senator DURBIN. If I might respond?

Senator FEINSTEIN. Please.

Senator DURBIN. Senator Feinstein, I want to agree completely with what Senator Craig just said, especially the operative phrase "to my knowledge," because we are in a position here where we cannot answer the most basic question, and it is this: In a Government of checks and balances, are you in Congress adequately supervising and monitoring the activities of the executive branch to make certain that there are no excesses? And the honest answer is we have not and we cannot.

Much of what is done under the PATRIOT Act is done in secrecy. The targets never know that they are being the subject of search and surveillance. In addition, there are gag orders that are put in place that really restrain everyone from disclosing what has occurred. You serve on the Intelligence Committee, as I did for 4 years. You know the cat-and-mouse game we play with those agencies trying to figure out exactly what is being done, hearing after weary hearing where little or nothing is said in an attempt to make sure that Members of Congress really do not know all the details and facts.

We need to respect our institution and our responsibility when it comes to checks and balances. The PATRIOT Act is, frankly, a large donation of our authority and responsibility to the executive branch without adequate safeguards there to protect individual rights and liberties. I think that is what is dangerous.

Senator FEINSTEIN. Let me ask a couple of specific questions on 215, on the John Doe roving wiretaps, on 802, and on delayed notice. Let me begin with delayed notice.

Despite some confusion, this section, while part of the PATRIOT Act, involves Title 18 and a much more traditional law enforcement technique. So-called sneak-and-peek warrants are an important law enforcement tool. My concern is that the catch-all section, which allows issuance of such a warrant when it would jeopardize an investigation, is unnecessary and may invite abuse. I would appreciate your views on this.

Senator DURBIN. Senator Feinstein, the SAFE Act eliminates that Section 802.

Senator FEINSTEIN. Pardon me?

Senator DURBIN. The SAFE Act would eliminate that 802 Section that you are concerned about.

Senator FEINSTEIN. Okay. Now, let me ask you about the definition of domestic terrorism. So it eliminates that as well?

Senator DURBIN. I would say that it amends it. Currently, the definition of domestic terrorism could include civil disobedience by political organizations. While civil disobedience is and should be illegal by its nature, 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 it is currently written. So we try to really bring it right back into the terrorism area, which was our focus in the PATRIOT Act, but not let it extend to any violation of Federal or State law, criminal law, which I think is a more expansive definition.

Senator FEINSTEIN. I think—

Senator CRAIG. Senator, I would also add that you and I lived through an era in our country in which civil disobedience at times grew to violence, and it changed the character of Government for a time. And it also created law as a result of it.

At the same time, we have to continually safeguard the right of civil disobedience for the purpose of political expression, and there is a line you have to draw, and we think that we have clarified that for this purpose.

Senator FEINSTEIN. I think, Mr. Chairman, that one of the things we might do is take a look at the definition of domestic terrorism. Some people think it is too broad and that it should be specifically narrowed.

Let me ask a question on 215, the so-called library provision. We have had testimony that the library provision has not been used with respect to libraries, but has been used with respect to the collection of financial records. What exactly does the SAFE Act do with respect to Section 215?

Senator DURBIN. Thank you. Senator Feinstein, this situation now under 215 allows what we think to be an overly broad and expansive search of records. Concerns have been expressed by librarians, but also by others, as to whether or not they would be forced to turn over records about many individuals, some of whom were not the target of suspicion, and thereby violate the privacy and disclose information that people did not believe would be readily disclosed except under criminal circumstances.

And so what we do is to say 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, requiring 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 the recipient the right to challenge.

So many times we heard the Department of Justice defending this provision, Section 215, saying that it was analogous to a grand jury subpoena. With the SAFE Act, Senator Craig and I draw the analogy tighter and say then let's live by that standard, if that is exactly as it should be, so that people know that they are the subject of such a search and that the Government specify that they are not going after everyone who checked a book out of the L.A. Public Library but, rather, specific people for whom they have identified some concern about the possibility of terrorism.

Chairman SPECTER. Senator Feinstein, your time has expired.

Senator FEINSTEIN. Thank you very much.

Chairman SPECTER. We have a very big second panel, six witnesses.

Senator KYL?

Senator KYL. Thank you, Mr. Chairman.

On that last point, the recipient, that is to say, the library or the hotel or whoever is being asked to supply records, has a right to challenge that and require the court process for a subpoena. Is that not correct? Under the existing law.

Senator DURBIN. No, that is not true.

Senator KYL. Why isn't it?

Senator DURBIN. They don't have the authority to challenge the order.

Senator KYL. They certainly do. It is a voluntary request for the records, and if they decide that they don't want to comply with it, they have a right to require—

Senator DURBIN. It is not a voluntary request, Senator. It is a court order. They are faced with producing the information.

Senator KYL. They have a right to contest the court order, do they not?

Senator DURBIN. I do not believe they do.

Senator KYL. Okay. We have a disagreement on that.

The people who are the subject of a search—

Senator CRAIG. Jon? Senator?

Senator KYL. Let me just ask this question: The people that are the subject of a search are not necessarily known before the records are divulged, are they?

Senator CRAIG. No.

Senator KYL. In other words, the point of the search is to find out who might have checked out a book on bomb-making. Isn't that correct?

Senator DURBIN. The point we are making is that by general principle, constitutional principle, the Government cannot say we are going to subpoena the records of everyone living in Yuma, Arizona, to find out what they have been reading, to see if among all those people we can find suspicion.

We live in a world—

Senator KYL. Do you know of any case where anybody has suggested that?

Senator DURBIN. But, you see—

Senator KYL. That is a red herring. The point of the business records, is it not, is to try to discover who might have checked into this hotel for the last three nights or who might have checked out a book on bomb-making, that kind of thing. You don't know necessarily the subject of your inquiry before you make it, do you? Go ahead, Senator Durbin.

Senator DURBIN. The point I am getting to, Senator, is that if you want to depart from the basic body of law which has governed us, probable cause before the Government goes forward, that would, in fact, violate the privacy of an individual based on that probable cause, which has always been our standard, then you would oppose the SAFE Act.

What we have said is you have to have some linkage here, and to argue that we don't know it has been violated is to state the obvious. Of course we don't. The Government is not forthcoming telling us how this is being used. We meet in closed session to talk about the possibilities of how it is being used. We do not have the tools to really decide whether there is an abuse. The checks and balances are not really—

Senator KYL. Let me ask you both this question: Do you believe that the same kind of authority then should be eliminated with respect to all of the other kinds of investigations that it already has been authorized for under our law, that terrorism is the only possible crime that should be eliminated from this—that terrorism should be the only crime for which this particular tool should not be available? Senator Craig?

Senator CRAIG. No, I am not suggesting that, nor do I believe the authority exists today to walk into a library and sweep the records. It does now under this Act. And I don't think it is a red herring, Jon, at all to suggest that you might get a rogue agent, not necessarily a rogue agent, who did just that and, therefore, found everybody in Yuma, Arizona, who checked out bomb-making and began private and secret investigations of why they did it.

Senator KYL. Okay. May I just ask then, to follow up on Senator Feinstein's question, do either of you have an example in any other context—because there are no examples in the context of terrorism—where this general business records authority has been abused?

Senator DURBIN. I would just say in response to that, if you want to follow the basic standard of probable cause or grand jury subpoena where they can be contested, where there is disclosure, where someone can say this is too far-reaching, then I think there is a safeguard built into the system. Such a safeguard does not exist when it relates to the PATRIOT Act, and that is the point we—

Senator KYL. So there are no examples either outside the PATRIOT Act or within the PATRIOT Act that either of you can cite where there was an overly broad request under the business record—

Senator CRAIG. Jon, I believe that is totally the wrong premise. I don't believe you wait until somebody has been dramatically injured before you re-establish—

Senator KYL. Okay—

Senator CRAIG. Now, wait a moment. I think it is tremendously important—

Senator KYL. My time is just about out.

Senator CRAIG. That is true—

Senator KYL. I understand the point that you are making—

Senator CRAIG. But what is important today is there is a perception across the land—

Chairman SPECTER. Senator Kyl—

Senator KYL. I just wanted to conclude my point here. The point of the sunset was to provide a testing period to see whether it worked, to see whether there were problems. In this particular area, because there have been no problems, it seems to me that the assumption underlying the sunset provisions ought to then move forward, which is, there being no problems, the Act should be reauthorized.

Senator DURBIN. Mr. Chairman, may I say a word?

Chairman SPECTER. Yes.

Senator DURBIN. This is cloaked in secrecy, and because of secrecy we cannot exercise the oversight we need to protect individual rights and liberties. And to suggest that because we cannot come forward and give you specific examples is to state the obvious. It is designed so that no one can come forward and give you these examples.

Senator KYL. May I just—I have to follow up on that. Isn't it true that in testimony before this Committee the Attorney General and other Federal law enforcement officials have testified that this particular provision as to libraries has never been used? So it is not secret. They have actually testified to that. And isn't it also true that under the PATRIOT Act we are required—that the Department of Justice is required to submit a report to Congress so that it is not cloaked in secrecy and we do know whether or not there has been an abuse?

Senator DURBIN. There has been a statement that it has not been used as to libraries, that is true. But it has been used some 35 other times.

Senator KYL. And we are aware of that, so it is not cloaked in secrecy, is my point.

Senator DURBIN. I would say to the Senator, we are aware of it in the most general terms. But notwithstanding the reputation and integrity of any Attorney General, we have usually said in Congress we are a separate, coequal branch which has the power and responsibility of oversight. We are giving that up when we do not have the information to really form an opinion and to hold the Government accountable.

Chairman SPECTER. Thank you very much, Senator Kyl.

Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman. I have a short statement that I would like to ask to be placed in the record.

Chairman SPECTER. Without objection, it will be made a part of the record.

Senator FEINGOLD. And I just want to say how pleased I am to be joining Senator Craig and Senator Durbin in forming the Bill of Rights Caucus to work to ensure that civil liberties are adequately protected in legislation like the PATRIOT Act.

Mr. Chairman, these two Senators and you, the Chairman, and the Ranking Member are just doing a tremendous service not only to the Committee and the Senate, but to the whole process of fighting terrorism by having these hearings. The conversations that are starting to occur around this table to me are exactly what is needed. And I would say to my colleague from Arizona, because he is such a hard-working and always prepared Senator, I hope you will let this process play out.

For example, on these things that just came up today, you know, I cannot prove all kinds of abuses any more than I think you can prove there haven't been any abuses. But that is not our task. As Senator Craig indicated, our responsibility now is to make sure that we fix this thing where it needs to be fixed, to make sure that future abuses don't occur, whether or not abuses have already occurred. And, you know, I see progress, for example, in the sneak-and-peek provisions, delayed notification—which was one of the reasons I originally opposed the bill.

Senator Feinstein for 2 years has indicated she has not heard or seen of any abuses of the bill. But she now sees, because she also always makes sure she studies things very carefully, that there is a catch-all provision that is too broad and cannot be justified in terms of the legitimate needs of sneak-and peek provisions.

So it is not a question of do we lay down the hammer and say nothing bad has happened and, therefore, we should just renew it? Or there have been all kinds of abuses and the question is: Is this particular catch-all exception justified? And I think it is becoming clear it is not. So it shouldn't be a victory for either side if we get rid of that provision. It is just fixing the bill.

The same thing goes for the library provision, Section 15. This has been an around-and-around thing. Yes, apparently Section 15 has not been used to command library records because many times library records have been obtained from librarians who have simply voluntarily given them. But the fact is library records have been obtained. That testimony was given under oath before this Committee. It is also perfectly possible that Internet records in the library were obtained under the national security letter provision. So it is not accurate to state that no library records have been obtained.

And the point that Senator Durbin was making I want to clarify here is if there is an ability to challenge under 215, I cannot find it. And the Senator from Arizona almost seemed to be saying that it would surprise him if there wasn't such a protection. So why don't we simply work together to make sure that there is an ability to challenge, a legitimate ability to challenge, and forget about who was right or wrong in the first place about it.

So I would simply urge—that is the kind of good-faith process I want to enter into here. I am not recommending repealing a single provision of the USA PATRIOT Act nor do I think the leaders here are. We simply want to put the protections that are needed.

So, Mr. Chairman, thanks for the opportunity to make those comments.

Chairman SPECTER. Thank you, Senator Feingold.
Senator Biden?

Senator BIDEN. I have no questions for the witnesses. I will have questions for the record, but I do not want to tie them up.

Chairman SPECTER. Thank you very much.

Senator Durbin, you had made a comment that the information in the closed session is not available to the public generally. Of course, it is available to you as a member of the Committee, and if other Senators wanted to have access to what went on in closed session, it would be my inclination to make that available to members. And when we Act on legislation and file a report, it would be my intention to give as full a picture publicly as we can at that time to what we know. If there are sources or methods or there is confidential information, we would respect that. But we would intend to do what we could to put that on the record. And we intend to proceed on these oversight hearings.

We thank you for the compliments, Senator Craig, about the Ruby Ridge hearings. You were an ad hoc member of that Committee. You were not on the Committee, but when you showed a real interest in it, I was the Subcommittee Chairman and invited you to attend. And as Senator Leahy has noted, that resulted in the change of the FBI rule on the use of deadly force, and Randy Weaver said that had he known he would have been treated so fairly by the United States Senate, he would have come down off the mountain. That is an oversight hearing 10 years old that has been repeatedly cited, practically solely cited as the oversight process, but this Committee intends to do a great deal more of that.

We thank you for coming.

Senator LEAHY. Could I just make one note, Mr. Chairman? We talk about—and as I said, there are many parts of the PATRIOT Act I like. I helped write or did write several parts of it and with others in a cooperative effort. But before we think this is the only thing we have for our security or the ability to get terrorist information, whether it is in what somebody's records have been in a library or anywhere else, we have always had the ability to have a grand jury subpoena. We have always been able to do that irrespective of whether the PATRIOT Act was there or not. And I think I just don't want—even though there are parts of this Act I support and parts of it that bring us into the digital age, for example, the modern age of law enforcement, let us not think that somehow the United States prior to the PATRIOT Act was undefended. I think it was far—I mean, it sort of overlooks the fact that we had hundreds of hours of tapes, for example, of people talking about terrorist acts that the FBI hadn't gotten around to translating prior to September 11th. We had a whole lot of other things we had available to us that we had gotten through the appropriate methods; we just had not connected the dots.

Chairman SPECTER. Thank you very much, Senator Leahy.

The exchange I think has been very fruitful. If we had this kind of floor debate as the exchange between Senator Kyl on one side and Senator Craig and Senator Durbin on the other, we might get farther in our floor debate. So at least we have the Committee hearings.

Before calling the second panel, Senator Biden, would you care to take 5 minutes for an opening statement?

**STATEMENT OF HON. JOSEPH R. BIDEN, JR., A U.S. SENATOR
FROM THE STATE OF DELAWARE**

Senator BIDEN. Yes, I will take a few minutes if I may, Mr. Chairman. As usual, thank you for holding this hearing.

Let me begin by suggesting that from my perspective, Mr. Chairman, as we approach this fourth anniversary of September the 11th, it is important we do everything in our power to identify and dismantle terrorist groups, but also find out what works and doesn't work and how well it works and doesn't work. And let me raise three quick points, if I may.

First, I believe the PATRIOT Act was a reasonable and necessary response to the terrorist attacks of 9/11. As I said before, no matter who was President, no matter who was in the Congress, there would have been mistakes made. There would have been things, looking back on it, we should do differently, and that is the context we should be looking at this.

I believe that when we passed this bill, it made sense. As a matter of fact, as far back as 1995 and 1996, I proposed similar provisions relating to the Oklahoma bombing case, that we should change the law similarly.

It simply did not make sense to me and it still does not make sense to me that law enforcement has certain tools that we can use against organized crime and drug gangs, but tools are not available to deal with terrorist organizations. And I said at the time what is good for the mob ought to be good for terrorists. Thus, I supported the PATRIOT Act because I think it meant moving toward a more level playing field involving terrorism with those garden-variety cases like drug and organized crime. And I also strongly supported its reauthorization.

But, secondly, I am aware that there are significant criticisms of the Act in recent years, and as I have said before, I believe much of the criticism is both misinformed and overblown. But that is not to say the critics aren't raising very legitimate concerns about how the administration has handled the war on terror.

I have been incredibly concerned with the decisions the administration has made involving the treatment of so-called enemy combatants, its decision to withdraw or withhold the application of the Geneva Convention to the hostilities in Afghanistan and the Justice Department's role in crafting what I believe to be misguided rules of interrogation. And I fear that these decisions make it more difficult to fight terror while placing our men and women on the ground in more jeopardy than they would otherwise have been.

I mention this because our ability to reauthorize the PATRIOT Act may be and is going to be made more difficult because of these misguided decisions, in my view, that the administration has made in other areas in the war on terror. And sometimes their actions there I find, as I am home and around the country, are confused with changes in Title 18, which they are not.

The third and final point that I would like to make, Mr. Chairman, is that we need to carefully consider whether we can improve the PATRIOT Act. I am open to considering whether we need to redefine or eliminate parts of the Act. I have been a Senator a long time, and like many of us here, I have been involved in every major piece of criminal and terrorist legislation in the past three decades.

And I have even cosponsored or written some of them. But every time we pass one of these laws, whether it was the Crime Control Act of 1994 or less significant pieces of legislation, I have said at the time I have urged their passage that we should go back and take a look at them a year or two later and find out whether or not what we passed has trenched upon anyone's civil liberties or, conversely, whether there are ways we can make it stronger to be able to deal with crime and terror. And so I think this is a logical process. We should be going back and thoroughly looking at what we did.

Today's hearing, in my view, is part of that process, and I think we have to ask a number of tough questions, not just about the 16 provisions which sunset at the end of this year, but the entire Act. And so I think we have to look at Section 215. Should we redefine it? Obviously, you all know 215 addresses the access to business records in terrorism investigations. Should it be redefined to make it clear that the same relevant standards which govern grand jury subpoenas also apply to these cases? I think maybe we should.

Section 206, which addresses roving wiretaps, should we make it absolutely clear that the Government cannot get a John Doe wiretap against an unknown person?

Section 213, which addresses sneak-and-peek search warrants, should that include reasonable future notification requirements to the target as we have long done with wiretap investigations against the mob and drug gangs?

So, in conclusion, Mr. Chairman, I believe these are just a few of the reasonable questions we need to ask and the potential tweaks and refinements to improve the credibility of the law without weakening the ability of the FBI or others to fight terrorism. So I am looking forward to the hearing, Mr. Chairman, and I thank you for calling it.

Chairman SPECTER. Thank you very much, Senator Biden.

While we have a number of Senators here, we have an agreement by Senator Leahy and myself to have a markup tomorrow on the asbestos bill, which will be in addition to our executive session on Thursday. We very much would appreciate attendance so that we could have a quorum and move ahead on that important bill. There are quite a number of amendments pending, and we are seeking to make modifications to accommodate members to the extent we can. So that will be held tomorrow morning at 9:30.

Chairman SPECTER. I want to call the second panel now: Former Congressman Bob Barr, Professor David Cole, Daniel Collins, James Dempsey, Andrew McCarthy, and Suzanne Spaulding. This distinguished panel has been called in alphabetical order. It is always hard to establish priorities among people with such outstanding records.

Our first witness is former Congressman Bob Barr, who represented the 7th District of Georgia in the U.S. House from 1995 to 2003. He has been engaged in many efforts on civil liberties, a member of the Long-Term Strategy Project for Preserving Security and Democratic Norms in the War on Terrorism at the Kennedy School of Government at Harvard. He had been United States Attorney for the Northern District of Georgia and also served as an official with the CIA from 1971 to 1978.

Nice to have you on Capitol Hill, Congressman Barr. The floor is yours for 5 minutes.

**STATEMENT OF BOB BARR, FORMER MEMBER OF CONGRESS,
AND CHAIRMAN, PATRIOTS TO RESTORE CHECKS AND BAL-
ANCES, ATLANTA, GEORGIA**

Mr. BARR. Thank you very much, Mr. Chairman. I appreciate yourself and the Ranking Member and the other members of this Committee, both those that are currently here and those that were here earlier at the beginning. And I know, as we always faced in the House, there are competing demands and floor action and people come and go from the Committee. But I also know that particularly members of this Committee, whether they are present for an entire hearing or not, pay very, very close attention to the materials that are submitted, the testimony that is rendered, and the issues involved. That has always been the hallmark of this Committee, and I appreciate the honor of being invited to play a small role in its deliberations on the USA PATRIOT Act today and in the weeks and months ahead.

I have listened to the testimony of the first panel, the two distinguished Senators, and the comments, questions, and dialogue by members of this Committee, and I think that the witnesses presented very, very eloquently the position that I endorse in terms of the need to pay very close attention to the USA PATRIOT Act, to conduct the oversight that is implicit in the provision of the sunset clauses in the legislation, to look very carefully at the ways in which the Act and its provisions have been used over the ensuing three and a half years or so since its enactment, and to look at possible problems. And, of course, one of the things that this Committee does look at is not simply bald acts of abuse with Federal legislation. We all know that abuse can be very insidious. It can be systematic. It can be very subtle. It may not even occur in order for this Committee to deem it necessary to take a look at powers granted to the Federal Government and say we think that these ought to be amended.

And that of course is explicitly why the Congress, in its wisdom, enacted as parts of the USA PATRIOT Act in 2001 the sunset provisions.

I do think that when one looks, particularly as a distinguished member of this Committee—and I had the honor of serving in its counterpart over on the House side for 8 years—I do think that from one's background, in my case in particular as both a United States Attorney for the Northern District of Georgia as well as having spent several years with the CIA and bringing a fairly comprehensive background to this debate, including my service in the House, I can say that I believe that in large measure, the PATRIOT Act, as Senators Craig and Durbin, as proponents and advocates and co-sponsors of the SAFE Act have indicated, has served this country well. But that is not to say that it is a perfect piece of legislation, an even if in fact the amendments proposed to the USA PATRIOT Act by the SAFE Act were enacted, I dare say probably it still would not be a perfect piece of legislation. It is constantly going to be, as it ought to be in our system of Government, a work in progress.

But I do think, Mr. Chairman, that the proposals contained in the SAFE Act are reasonable, they are modest. In my view again, as a former U.S. Attorney, as a former official with the CIA, do not remove in any way, shape or form, important powers that the Government needs to fight serious acts of criminal activity, including acts of terrorism. The amendments proposed, for example, to the so-called sneak-and-peak powers contained in section 213 of the PATRIOT Act clearly recognize that this is a power that the Federal Government needs from time to time, but it ensures that that need remains the exception and not the rule, and it clearly contemplates that there will be circumstances, should be circumstances under which the Federal Government can use the extraordinary remedy or take the extraordinary step of conducting a search of a person's home or business without providing contemporaneous notice, when to do otherwise would seriously endanger national security.

That is the theme, Mr. Chairman, that underlies all of the various changes proposed in that modest piece of legislation called the SAFE Act. I commend those members of this body and their counterparts in the House who have already endorsed this legislation. I commend it as one of the pieces of legislation or one of the vehicles that the Committee might carefully scrutinize in its efforts to ensure that we always maintain that proper balance between the Bill of Rights and the need to fight acts of terrorism and other serious criminal activity.

I have submitted and would ask that my entire written comments be included in the record, and I stand ready to provide any additional written materials or answer any questions that the Committee or its distinguished members might have.

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

Chairman SPECTER. Thank you very much, Congressman Barr, and your full statement will be made a part of the record, as will all statements be made a part of the record.

We turn now to our second witness who is Professor David Cole, Professor of Law at Georgetown University, had been staff attorney for the Center for Constitutional Rights, and had served as a law clerk to a very distinguished Federal Judge, Arlen Adams, who happens to be a Philadelphian.

Welcome, Professor Cole, and we look forward to your testimony.

**STATEMENT OF DAVID COLE, PROFESSOR OF LAW,
GEORGETOWN UNIVERSITY LAW CENTER, WASHINGTON, D.C.**

Mr. COLE. Thank you, Chairman Specter, Senator Leahy, members of the Committee, for inviting me here to testify.

I want to make two points in my oral testimony. The first is that an inquiry into the PATRIOT Act ought to be the beginning, not the end, of congressional oversight of the executives carrying out the war on terrorism and particularly of the civil liberties abuses that have occurred therein.

The second point I want to make is that the worst provisions of the PATRIOT Act are by and large not those sunsetted, but other provisions that are not subject to sunset, but nonetheless deserve

your attention, namely the immigration provisions and the material support provisions.

So first with respect to the first point, that this should be the beginning, not the end. Defenders of the PATRIOT Act often complain that the PATRIOT Act gets criticized for more than it deserves, and I think there is some truth to that because many of the worst abuses of civil liberties that have been carried out by the Bush administration in the war on terror have been carried out outside the PATRIOT Act. A national campaign of ethnic profiling and a mass roundup of foreign nationals carried out outside of the PATRIOT Act, 80,000 people called in for special registration simply because they came from Arab and Muslim countries, 8,000 sought out for FBI interviews simply because they came from Arab and Muslim countries, 5,000 by the Government's count detained in preventive detention measures, almost all of them Arab and Muslim. And of these people not one today stands convicted of a terrorist crime. Zero for 5,000, zero for 8,000, zero for 80,000. But that is not with respect to the PATRIOT Act.

The Enemy Combatant Authority, the Attorney General regulations that allow the FBI to spy on religious services without any suspicion of criminal activity, data mining developments, and of course torture. All of these are serious concerns that arise outside of the PATRIOT Act. That does not mean however that you should take the PATRIOT Act any less seriously. It simply means that you should take the other abuse equally seriously.

The courts, to my mind, have played a very important role in checking the administration. They have ruled against the administration on the enemy combatants, on military tribunals, on the PATRIOT Act itself, on closed immigration hearings, on the refusal to divulge documents regarding the torture scandal. I think Congress also has a responsibility to check the administration.

The second point I want to make is that the worst provisions of the PATRIOT Act are not those subject to sunset. The immigration provisions allow for deportation of individuals for wholly innocent association with any group that we have designated as a bad group, regardless of the individuals' conduct in connection therewith. They allow for the exclusion of foreign nationals based on pure speech, pure speech. No conduct, no concern about threats, pure speech. They allow the Attorney General to detain foreign nationals without charges, and without showing that there is any basis for their needing to be detained.

The Civil Liberties Restoration Act has been introduced to try to respond to some of these abuses and the other immigration abuses that I laid out earlier, but it has not even gotten a hearing. And instead what is Congress doing? It is about to pass, very likely today, maybe tomorrow, the Iraq Supplemental Bill in which there is a provision which dramatically expands the scope of the immigration terrorism grounds to essentially resurrect the McCarran-Walter Act. Under this law you will be deportable if you had any association at any time in your life with any organization that ever used or threatened to use a weapon period. There is no defense to show that you had did not take part in the violence. You are deportable even if your father engaged in that, was a member of such a group.

So Nelson Mandela's child, if he has a child, would be deportable from this country. People who supported the Israeli military, the Palestinian Authority, the African national Congress, all deportable regardless of whether their support actually furthered any illegal activity.

That radical expansion is being carried out without any consideration by this Committee, without any open debate. It was put in by Senate conferees in conference.

So if anything, the abuses that we have seen since 9/11 in the immigration area should call for more oversight and more limitations on congressional power. Instead what Congress is about to do is to give the administration essentially a blank check.

I only have a few more moments I will leave for questions. The other two aspects I think raise very serious concerns outside of the sunset provisions, and those are the criminalization of pure speech in the Material Support Statute, which has been struck down in a case that I am handling, and the authority to freeze assets of any entity in the United States without showing that they engaged in any violation, and then to defend that action using secret evidence in court denying the entity any chance to defend itself.

Thank you very much.

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

Chairman SPECTER. Thank you, Professor Cole.

Our next witness is Daniel Collins, Partner in the Los Angeles Office of Munger, Tolles and Olsen. He had served from June of 2001 to September of 2003 as Associate Deputy Attorney General, and had been the Department's Chief Privacy Officer. A graduate of Harvard College and Stanford Law School, he clerked for Circuit Judge Nelson and Supreme Court Justice Scalia.

Thank you very much for joining us, Mr. Collins, and we look forward to your testimony.

**STATEMENT OF DANIEL P. COLLINS, MUNGER, TOLLES AND
OLSEN, LLP, LOS ANGELES, CALIFORNIA**

Mr. COLLINS. Thank you, Chairman Specter. Good morning Senator Leahy and distinguished members of the Committee. I am grateful for the opportunity to testify here today on this important subject.

Three-and-a-half years ago the USA PATRIOT Act was signed into law with overwhelming support in both houses. 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 Committee is well aware, some 16 provisions of Title II of that Act are scheduled to expire at the end of this year absent action by the Congress. In my view, these 16 provisions should be made permanent because today, as in 2001, they remain appropriate tools in the war on terror. I have addressed each of those 16 statements as well as Section 213, which is not subject to sunset, in my written statement, and I will focus in my oral remarks on three of them, Section 206, 215 and on Section 213.

With respect to Section 206, which deals with the issue of roving wiretaps, the change that is actually made by the PATRIOT Act itself is quite modest, and I think when you compare it to the regime of Title III, you will see that there is a critical difference that I think renders unnecessary the changes that would be made by the SAFE Act to the FISA roving wiretap authority. 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." That critical phrase was not added by the PATRIOT Act, but by the Intelligence Authorization Act for Fiscal Year 2002, and that amendment is therefore not subject to a sunset.

The provision that the PATRIOT Act added was a requirement that you do not necessarily have to specify, if not known in advance, the actual wire service provider. Rather you could have an order that whatever service provider became relevant would have to provide the assistance that is required.

Moreover, both the PATRIOT Act and the change that was made by the Intelligence Authorization Act leave in place the provision of Section 105(a)(3)(B) of FISA, which 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. What that means is that even when it cannot be specified in advance what particular facilities and places will be surveilled, the Government under FISA 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 that probable cause determination.

There is an analogous requirement to the one I just described in FISA in Title III, but Title III's roving wiretap provision waives that requirement. FISA does not. That critical difference provides an additional safeguard in FISA that I think has been overlooked in the analogy that the SAFE Act appears to attempt to draw between Title III and FISA, and I think renders the balance that is already struck by the PATRIOT Act on this subject a different one from Title III, but nonetheless an adequate one.

With respect to Section 215, this is, as many have noted, an effort to provide on the counterintelligence side an analog to the ability to get business records on the criminal side through the use of grand jury subpoenas. There has been an acknowledgement by the administration, the Attorney General in his recent testimony, that this provision could benefit from some clarifications. We have already seen in the discussion this morning a dispute over whether or not a court challenge to an order by a recipient of such an order is authorized. That could be clarified. That is a subject that is addressed in the SAFE Act. I think that the SAFE Act though in specifying that raises a number of issues that I think need careful study.

For example, the SAFE Act would impose an automatic stay on compliance with the order pending the challenge, and automatic stays are not typical in many contexts. It is not clear that that

should be the case here. Also the analogy to the use of CIPA in the civil context is something that I think needs very careful study.

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

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

Our next witness is Mr. James Dempsey, Executive Director for the Center for Democracy & Technology. He is currently engaged in subject matters of privacy and electronic surveillance issues, and heads CDT's International Project. He had been Deputy Director for the Center for national Security and had been Assistant Counsel for the House Judiciary Subcommittee on Civil and Constitutional Rights.

Thank you for joining us, Mr. Dempsey, and we look forward to your testimony.

**STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR,
CENTER FOR DEMOCRACY & TECHNOLOGY, WASHINGTON,
D.C.**

Mr. DEMPSEY. Good morning, Mr. Chairman, members of the Committee. Thank you for the opportunity to testify today. From this kind of detailed and objective inquiry and dialogue we can attain the balance that was left aside in the pressure and emotion of the weeks immediately after 9/11.

In CDT's view, Mr. Chairman, there are few if any provisions in the PATRIOT Act that should sunset. The question before us is what checks and balances should apply to those powers. In our view, every provision of the PATRIOT Act that is of concern can be fixed, preserving the investigative tool, but subjecting it to appropriate standards and judicial and legislative oversight.

In order to understand what is right and what is wrong with the PATRIOT Act, consider the key protections traditionally surrounding Government access to information under the Fourth Amendment.

First, as a general rule, searches and seizures and access to private data should be subject to prior judicial approval based on some factual predicate. Second, a warrant or subpoena must describe with particularity the items to be seized or disclosed. Third, individuals should have notice when the Government acquires their personal information, either before, during or after the search. And finally, if the Government overreaches or acts in bad faith, there should be consequences, including making sure the Government does not use the information improperly seized.

These components of a Fourth Amendment search—judicial approval, particularity, notice and consequences for bad behavior—are independent. When it is necessary to create an exception to one, that does not justify a blanket exception to all four. However, too often in the PATRIOT Act, when the Government had a good argument for dispensing with one or another of these protections, it insisted that Congress eliminate all of them, leaving many of the powers in the PATRIOT Act with none of the traditional checks and balances.

The issue has been raised time and again about abuses—and I wish Senator Feinstein were here because I would like to gently

correct Senator Craig and Senator Durbin. I think there is evidence of abuses now, despite the secrecy surrounding the Act.

Section 215, sneak-and-peek: the FBI has used that to break into a judge's chambers secretly in a judicial corruption case, to break into an office in a Medicare fraud investigation. Now, these are permitted within the terms of the legislation, but I think those are abuses. I think those are not the kind of violent crime or terrorist crime for which a secret search is appropriate. The Justice Department has admitted that in one case the search was delayed for 406 days. I think that is an abuse, a delayed notice for 406 days under the PATRIOT Act.

Section 805, material support: The Government charged with material support a person who was posting on his website material that it turned out was also posted on the website or linked to from the website of one of the prosecution's witnesses. That came out in trial. The jury acquitted that person after he had spent a year and a half in jail. I think that is an abuse.

The national Security Letter provision has been declared unconstitutional by a Federal District Court Judge. I do not know if you would call that an abuse or not, but a provision of the PATRIOT Act has been declared unconstitutional.

The Mayfield case offers an interesting window. That was a criminal case, and yet they used a sneak-and-peek secret search under FISA, with no notice. Ultimately, the case blew up in the Government's face partly because the Spaniards kept saying, "You got the wrong guy." If the Spaniards had not been saying "He's the wrong guy," it is very possible that Mayfield would have gone to trial based upon the testimony of an FBI fingerprint expert.

Now, one of the Justice Department's central arguments is that the PATRIOT Act standard of mere relevance under the FISA pen register provision, Section 215, and the national Security Letters, is just like the standard for grand jury subpoenas in criminal cases. This argument overlooks the fundamental differences between criminal investigations and intelligence investigations. If the Government wanted to use grand jury subpoenas against terrorists, they could since terrorism is a crime. But intelligence investigations have additional powers and features which need countervailing protections. They are much broader. They are not cabined by the criminal code. They can collect information of First Amendment activities. They can even be based on First Amendment activities in part against U.S. citizens. They are secret.

In the criminal context, the trial is the big show. And as you know, Mr. Chairman, the prosecutor's whole conduct is put under scrutiny there. None of that happens in the intelligence case, unless there is a trial. Therefore we need countervailing protections to account for that.

Mr. Chairman, I will be happy to work with you and members of the Committee on the SAFE Act. As Senator Biden referred to, how can we fix this legislation? Of course, mistakes were made. It is inevitable. Let us go back and look at it and put some of these checks and balances back in.

Thank you, Mr. Chairman.

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

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

Our next witness is Mr. Andrew McCarthy, Senior Fellow at the Foundation for the Defense of Democracies here in Washington. Had been a Federal prosecutor in the U.S. Attorney's Office for the Southern District of New York, where he had some notable convictions leading to prosecution against the terror organization of Sheik Omar Abdel Rahman, who was convicted of conducting a war or urban terror in the United States, and also led the litigation over crucial confession evidence which helped secure convictions in the bombings of the American embassies in Kenya and Tanzania. A prolific writer on a wide variety of subjects.

We thank you for coming in today, Mr. McCarthy, and the floor is yours.

**STATEMENT OF ANDREW C. MCCARTHY, SENIOR FELLOW,
FOUNDATION FOR THE DEFENSE OF DEMOCRACIES, WASHINGTON, D.C.**

Mr. MCCARTHY. Thank you, Mr. Chairman, and members of the Committee.

Senator Specter, you mentioned my background in terrorism cases, and I think to the extent I have anything relevant to say to the Committee today it is from those trenches, the front lines where the war on terrorism is actually fought, and it is from the perspective of those trenches that I thank this Committee and the entire Congress for its tradition of strong bipartisan support in ensuring that our law enforcement and our counterterrorism officials at the FBI and the Justice Department have the tools that they need to protect our national security.

It was that tradition that impelled members of both houses of Congress and both parties to enact the USA PATRIOT Act by overwhelming margins. It was a good potential idea back then.

Nearly four years later, with no attacks on our homeland since 9/11, even though we know our enemies are desperately trying to attack us, I think we can say confidently that it is now a good proven idea.

It has been a crucial ingredient in the American people's inoculation from the perilous disease that is terrorism and it remains good, relatively pain-free protection that we badly need. Just as we do not eliminate or water down vaccines when we are fortunate enough to go three or four years without a major outbreak of disease, it would be unwise and I think dangerous to eliminate or water down the major protections of the PATRIOT Act, and I am relieved and happy to see that for the most part the consensus seems to be that almost all of the PATRIOT Act, but for a few finite areas of disagreement, should be preserved and will be preserved.

If I may, I would like to try to make two points this morning. The first concerns reasonableness. The demands of national security are undoubtedly intentioned with our freedoms. The tension is not always the same, it ebbs and flows. If you believe as I do that we are in a real war that presents real threats from murderers who play by no rules, the tension is raised. It calls for tolerable curbs on our liberties and tolerable intrusions on our privacy. If you believe that the threat is overstated or being used pretextually to ad-

vance other agendas, then there is a natural inclination to emphasize our freedoms and our privacy, and I think many of my thoughtful colleagues have done just that.

The genius of our system is that even if we never reach consensus on those things—and I doubt that we ever will—we are guided by a rule of reason. The Fourth Amendment asks one core question: is Government acting reasonably? It venerates privacy but it implicitly acknowledges that Government's highest burden and highest responsibility is to protect our collective security. It rejects rigid prior restraints on either Government action or freedom. It says do what is reasonable.

The PATRIOT Act is reasonable. It strikes a proper balance between the demands of public safety and private freedom. If it were unreasonable, you would have a record to show that, and after four years, you do not.

I would submit that it is not reasonable to water down or eliminate provisions on the basis of hypothetical fears, and that is the major part of the debate that we have had over the PATRIOT Act, most of the challenges have been hypothetical.

With the few remaining moments I have, the other thing I would like to stress this morning briefly is to urge this Committee to reject the premise that is at the heart of many of the reform proposals, which is that honorable people will behave dishonorably. The people on the front lines are not perfect by any stretch, they are in a pressure-packed job to protect us, they are forced to make hard judgment calls, and inevitably mistakes get made. I know. I made my fair share.

But they are honorable. They are Americans who believe in civil rights. They take an oath to uphold the Constitution. They do not have a voyeuristic interest in spying on the private affairs of their fellow Americans. What is more, as a practical matter, they would not have the time even if they did have the inclination.

As all of the investigations of intelligence failure demonstrate, they have enough of a challenge reading and digesting those things that we desperately want them to read and digest. The notion that they are Big Brother seeking to monitor our every move is not reality. Again, it is not reasonable.

The best way to handle errors or over reaching, and those are inevitable, is oversight by this Committee and others. It is not to erect barricades against effective and necessary intelligence collection.

Thank you, Mr. Chairman.

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

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

Our final witness—it is arranged alphabetically—is Ms. Suzanne Spaulding, who has an extraordinary record, now Managing Director of the Harbour Group. She served as Executive Director of two congressionally mandated committees, the national Commission on Terrorism and the Commission to Assess the Organization of Federal Government to Combat the Threat of Weapons of Mass Destruction, where former CIA Director John Deutch, chaired it and I served as the Vice Chairman. And she worked as Deputy Staff Director and General Counsel for the Senate Select Committee on

Intelligence, and she also worked as Assistant General Counsel for the CIA. Quite a portfolio with one exception, where she was my Legislative Director and Senior Counsel, I believe, at the start of her now illustrious career.

Ms. Spaulding, thank you for joining us.

**STATEMENT OF SUZANNE E. SPAULDING, MANAGING
DIRECTOR, THE HARBOUR GROUP, LLC, WASHINGTON, D.C.**

Ms. SPAULDING. Thank you, Mr. Chairman, Senator Leahy, members of the Committee. I appreciate this opportunity to participate in today's hearing on the USA PATRIOT Act and the legal framework for combating international terrorism.

Let me begin by emphasizing that I have spent over 20 years working on efforts to combat terrorism, starting in 1984 when I had the privilege to serve as Senior Counsel to then Committee member and now Committee Chairman, Senator Arlen Specter, who, as many of you know, in 1986 introduced and guided to passage the first law to grant extraterritorial jurisdiction over terrorist attacks against Americans abroad.

Over the succeeding two decades, in my work at the Central Intelligence Agency, at both Senate and House intelligence oversight committees, and with the two independent commissions on terrorism and weapons of mass destruction, I have seen how the terrorist threat has changed from one aptly described in the mid 1980s by Brian Jenkins' remark that "terrorists want a lot of people watching, not a lot of people dead," to one that is now more aptly characterized by former DCI Jim Woolsey's observation that "the terrorists of today don't want a seat at the table, they want to destroy the table and everyone sitting at it."

There is no question that today we face a determined set of adversaries bent on destroying American lives and our way of life. The counterterrorism imperative is to deny the terrorists both of these objectives. Evaluating how well the USA PATRIOT Act, as enacted and as implemented, satisfies this counterterrorism imperative is the fundamental task for this Committee, for the Congress as a whole and for the American public.

One of my greatest concerns about the USA PATRIOT Act and other changes in the law over the last several years is the way in which intrusive criminal investigative powers have migrated into the careful legal framework we had established for domestic intelligence collection, which is largely governed, as you know, by the Foreign Intelligence Surveillance Act or FISA. Tearing down the wall that hampered the sharing of information between intelligence and law enforcement was absolutely essential and I supported it. Nevertheless, there are significant differences in the way that information is collected in intelligence operations as opposed to criminal law enforcement investigations, differences that require particularly careful oversight of any new powers granted in the intelligence context.

Intelligence operations present unique risks. They are by necessity often wide ranging rather than specifically focused, creating a greater likelihood that they will include information about ordinary, law-abiding citizens. They are conducted in secret, which means abuses and mistakes may never be uncovered, and they lack

safeguards against abuse that are present in the criminal context where inappropriate behavior by the Government could jeopardize a prosecution. These differences between intelligence and law enforcement help explain this Nation's longstanding discomfort with the idea of a domestic intelligence collection agency.

Because the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigations should be no broader or more inclusive than is absolutely necessary to meet the national security imperative, and should be accompanied by rigorous oversight by Congress, and where appropriate, by the courts.

Unfortunately, this essential caution was often ignored in the FISA amendments contained in the PATRIOT Act. Changes to FISA were often justified with arguments that this authority is already available in the criminal context, and "if it's good enough for use against drug dealers, we certainly should be able to use it against international terrorists." But in the FISA amendments in Sections 214 and 215 of the PATRIOT Act, for example, we moved from the criminal requirement that information demanded by the Government be "relevant to a criminal investigation" to a FISA requirement that information be "relevant to an investigation to protect against international terrorism." Consider this term. It does not say an investigation into international terrorism activities, which would at least mean there was some specific international terrorism activity being investigated. No. Instead it says, "an investigation to protect against international terrorism." Imaging if the FBI was engaged in an investigation to protect against bank robbery. What does that mean? Just how broad is that scope? Whose records could not be demanded as relevant to an investigation to protect against terrorism?

Mr. Chairman, let me conclude by noting that we often say that democracy is our strength. A key source of that strength stems from the unique relationship between the Government and the governed, one based on transparency and trust. Intelligence collection imperatives challenge those democratic foundations and demand rigorous oversight.

These hearings and your willingness to consider whether provisions adopted in haste at a time of great fear should be renewed or modified, will contribute significantly to restoring the necessary public confidence that the Government is protecting both American lives and America's way of life.

Thank you for your work and for this opportunity to participate today.

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

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

We now turn to questions from the panel, limited to 5 minutes each.

I start with you, Mr. McCarthy. Your outstanding record on prosecuting terrorism and securing key convictions is really extraordinary.

Mr. MCCARTHY. Thank you.

Chairman SPECTER. And my question to you goes to the use of the so-called roving wiretap. When we considered the PATRIOT

Act late one Thursday night, Senator Feingold offered an amendment that would have required the person implementing a roving FISA order to ascertain the presence of the target before conducting the surveillance. I was one of 7 Senators who supported the amendment out of concern for the basic issue, but also out of concern for, candidly, the short shrift that the amendment got before we had a tabling motion.

Is that so-called roving wiretap really important for battling terrorism?

Mr. MCCARTHY. The roving wiretap is crucial for battling terrorism. I do not want to suggest that I think that that amendment would have been unreasonable. I think it is unnecessary and it is sort of a belt and suspenders type add on if you take a look at the roving wiretap statute as a whole.

And what I would stress to the Committee is that in many parts of the PATRIOT Act what critics have said about it is that what we need here is more judicial oversight. Here is a place where I would suggest that you should trust judicial oversight. The Government cannot get a roving wiretap unless they establish probable cause that is sufficient to at least describe a known person, not necessarily identify the person, but give an adequate enough description that you could find probable cause that the person was doing the predicate activities of the statute, and that the person would be using instruments—

Chairman SPECTER. Thank you, Mr. McCarthy.

I want to ask Ms. Spaulding a question, and I want to come to Mr. Barr. I would like to ask all the members questions, but we have very limited time.

Ms. Spaulding, when you had commented about relevancy, my question to you goes to business records and a discussion we have been having about having a higher standard. True, nobody has sued them for library records or medical records, at least up to this point. But do you believe there ought to be a standard pretty much equivalent to probable cause to obtain a search warrant before going in to get business records?

Ms. SPAULDING. Mr. Chairman, I think at a minimum we ought to consider a higher standard for records that implicate First Amendment activity, and probable cause might be the appropriate standard there.

I also think that Section 215 could potentially stand a clarification that it applies only to business records. As I read it now, it applies to any tangible thing held by anyone. It is often justified by citing court opinions related to third-party records, and I think most people assume that what it attempts to reach is business records, but it does not specify that. I think there are clarifications that would help.

Chairman SPECTER. Thank you.

Congressman Barr, you testified before the House Committee on the issue of delayed notice, so-called sneak-and-peek, and we are searching for a time limit as to what would be reasonable to impose. There is one case where a court in Illinois imposed a 7-day time limit, and that resulted in having the Assistant U.S. Attorney seek 31 extensions over an 8-month period. We are going to take a close look at that case to see why he had 31 extensions, or why

if the matter would warrant 31 extensions and he got 31 extensions, or at least 30, that there would be so many.

But based on the experience you have had, which is extensive, how would you craft a time limit on the so-called delayed notice matters?

Mr. BARR. I think that the case that the Senator cites illustrates a couple of things, one, that generally speaking, even if on the surface a procedure appears burdensome, it probably really is not, and courts are very much inclined—and this is compatible with my experience as a U.S. Attorney—courts are very much inclined to grant governmental requests in this area, and that is because, one, the authority that the Government has is rarely abused. It is sometimes, but rarely. And courts show great deference to the prosecutors when they come to the court and ask for an authority or for an exception such as sneak-and-peek.

Chairman SPECTER. Congressman Barr, I have one more question for Professor Cole.

Would you repeal the PATRIOT Act entirely?

Mr. COLE. No, I would not.

Chairman SPECTER. Thank you.

Senator Leahy.

Senator LEAHY. I agree with Professor Cole. But I do have some problems with some parts of it.

And in the hearing before the House Terrorism and Homeland Security Committee, Congressman Barr, you were asked about the PATRIOT Act sunset provision, and you said: I am somewhat mystified by a lot of my former colleagues, and your current colleagues are so afraid of a sunset provision, particularly those of us who are conservative about many issues. I do not think that we would be here today, I do not think that these hearings would be convened at this point were it not for the sunset provisions. It is a very important provision that liberals and conservatives alike ought to embrace.

Obviously, as one of the authors of that sunset provision, I agree with you. The administration wants to do away with the sunset authorities, make them permanent. Is there a problem if they are made permanent rather than maybe extending a sunset provision?

Mr. BARR. I think that it would be problematic. These are very extraordinary powers that we are speaking of here. Even though the Government has shown an increasing propensity to use these extraordinary powers in what I think a number of instances are not extraordinary cases, they are extraordinary powers, and I think Congress ought to very, very zealously guard against making them permanent. It is, as a practical matter in both houses of the Congress, as the Senator I think would agree, much more difficult to enact legislation that corrects a problem if there is not a sunset provision. That provides at least a guaranteed vehicle for the Congress to take advantage of.

Senator LEAHY. Thank you.

Ms. Spaulding, you have had probably as extensive a background in intelligence matters and the preventive work that intelligence can do, and others, and certainly in this area. Do you think the sunset authority should be made permanent, extended or some

combination, and were they worthwhile having them in there in the first place?

Ms. SPAULDING. I will say that when the PATRIOT Act was first enacted with the sunset provisions, it was not clear to me that they would—how effective they would be. But in hindsight I think they were brilliant. I think it is absolutely the case that we would not have had the level of public discussion and debate, the intense focus by Congress had those sunset provisions not been there. I think they have been incredibly important.

Having said that, I would not like to see sunset provisions, clearly, take the place of making changes and modifications today that we now know need to be made. And one area where I feel particularly strongly about that is the lone wolf provision, which in some ways makes the most compelling case for extending the sunset because it was so belatedly enacted, just last year, but nevertheless, I think has some real problems that should be addressed now.

Having said that, I think this is a brave new world for us, we are finding our way, and sunset provisions make a lot of sense in this context.

Senator LEAHY. You, like many of us on this Committee, have handled intelligence matters including code word clearance and those things. Do you believe that more information on the use of surveillance powers could be shared with the Congress and actually with the public without jeopardizing national security?

Ms. SPAULDING. I think a great deal more information could be shared with Congress certainly than was made available when I was on congressional staffs. I do not have insight into all that is shared today, but I think, for example, even the content of FISA applications, of current FISA applications, could be shared with at least Committee members.

Senator LEAHY. Let me go into that because in prior Congress, as I introduced the Domestic Surveillance Oversight Act—Senator Specter and Senator Grassley have been co-sponsors of that—I felt it was intended to shine more light on what is going on in FISA, requires, for example, reports on U.S. persons targeted under FISA, at how often FISA is used for criminal courts, to give Congress more information on how the FISA courts operate, and a review of constitutional questions back in November 2003. Representative Barr said he would support it. Would you support this increased reporting that is contained in the Domestic Surveillance Oversight Act that Senator Specter, Grassley and myself and others have—

Ms. SPAULDING. I would, Senator. I do not see any harm to national security, and I think that, while the numbers do not tell the public a great deal, they can at least serve as a prod to heighten oversight.

Senator LEAHY. Thank you.

Actually, I do have one question for Mr. Dempsey. We do have this public library question. How do you ensure against sort of Big Brother snooping that has generated so much discussion, without making librarians safe havens for terrorists, as Director Mueller has suggested?

Mr. DEMPSEY. Well, I think that at the end of the day, there is no category of records that the Government should not have the

power to get, but the question is, what are the standards, what are the checks and balances? Right now under Section 215 there is no factual showing, there is no specificity, there is no notice ever to the person whose records are provided to the Government. While there is clearly a need for secrecy during the conduct of intelligence investigations, I think we need to counterbalance that with a meaningful, truly meaningful judicial review based upon a factual showing and some specificity.

Senator LEAHY. Thank you.

Thank you, Mr. Chairman.

Chairman SPECTER. Senator Kyl.

Senator KYL. Let me ask, Mr. Collins, about that last point in your written testimony. You refer to the fact that Section 215 actually contains more protections than the rules governing grand jury subpoenas. Why do you not elucidate on that a little bit?

Mr. COLLINS. Yes. In my testimony I specified a number of the different elements that there are under Section 215 to getting a court order under FISA for business records. First, a court order is required. In a grand jury subpoena the AUSA pulls out a grand jury subpoena, types it up and signs it. The court is not merely a rubber stamp. The statute explicitly states that it can modify the order, and indeed, the Department, in its recent report about orders under 215, has indicated that that power of modification has in fact been used.

The statute has a narrow scope, can be used in an investigation of a U.S. person only to protect against international terrorism or clandestine intelligence activities, cannot be used to investigate domestic terrorism, and provides explicit protection for First Amendment rights. It is not possible, as I believe someone asserted this morning, to go into a library and just say, "I want to see who checked out a particular book" that has no particular significance, not a book on bomb making. That is an order that would be predicated on First Amendment rights in violation of 215 as it exists today.

Senator KYL. And you further note that the standard established in the SAFE Act is that this authority could only be authorized—and I am quoting now—"if there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power, an agent of foreign power," which you described as too narrow a standard. Why do you believe that?

Mr. COLLINS. There has been discussion about whether there can be refinement of the standard here. I think that reasonable people can agree, or can differ on that question. For example, the word "relevance" actually does not appear in 215. That could be added in. But to raise it to the level of reasonable suspicion is too high. Say, for example, you know that a particular document has details about water supplies in a particular area, and it is a highly arcane document that was in Federal depositories, and you know that there was an interest in that particular dam, and you want to know who may have consulted the details that were available in Federal depositories. You could not do that. You could not get those records absent making a further showing that those records would pertain to a person who was suspected to be a foreign agent.

So it requires a higher showing. You could not just get the set. If you knew that five people had consulted those records you could not get all five without making a showing as to each five of them.

Senator KYL. Let me just ask you one final question. There has been some discussion of the delayed notification on the search warrants. Does that not occur with judicial review, and does the judge not put the limitations on there that he deems appropriate in a particular case?

Mr. COLLINS. Yes. Pre-existing case law seemed to have developed this presumption of a 7-day limit. That was not codified into 213. It allows each judge who authorizes it to set what he or she believes is the appropriate limit for the initial authorization and for the extensions, depending on the showing that is made in a particular case.

Senator KYL. So what would the Government ordinarily have to show as a justification to the court for the delayed notice?

Mr. COLLINS. There are five grounds specified for grounds for delayed notification. The SAFE Act, at least in the version now in the 109th Congress, the difference only comes down now to one ground. There is now agreement on preserving in full the other four grounds, and it is just the ground over seriously jeopardizing an existing investigation.

Senator KYL. What is your view on that?

Mr. COLLINS. I believe that that should be preserved as a ground. The Department has given a number of examples primarily in the context of what might be called spinoff investigations, where you are investigating one particular organization for one thing and then you realize that there is another collateral activity, there is credit card fraud or something. You want to intercept a package that is being shipped either to verify what is being shipped or to pursue further leads on that. But if you were to give the notification on the spinoff investigation, you would then tip off the larger investigation, and to force people to the choice of either, well, we will just ignore what we now know is a second criminal activity, seems I think too high a cost and the judicial supervision should be sufficient.

Senator KYL. Thank you.

Chairman SPECTER. Thank you very much, Senator Kyl.

Senator Feingold.

Senator FEINGOLD. I thank the panel and let me first ask if Mr. Dempsey wanted to respond to the point Mr. Collins was making?

Mr. DEMPSEY. I thought that the example that he gave about the rare document and a dam and the document had some information about the vulnerability of the dam and that it was known that people were interested in attacking that dam. I think that is specific and articulable facts.

Senator FEINGOLD. Thank you. That is what I assume was the point you wanted to make, one I would have made. Thank you very much.

Ms. Spaulding, the so-called lone wolf or Moussaoui fix became law last year as part of the Intelligence Reform and Terrorism Prevention Act, but it sunsets at the end of a year. I actually raised serious concerns about the lone wolf provision when it came through this Committee, and argued that it was an unnecessary

and possibly unconstitutional expansion of FISA. I also joined Senator Feinstein in offering an amendment to deal with the lone wolf problem by way of essentially a permissive presumption that would allow a FISA warrant to be issued in certain cases. You have had a lot of experience with FISA, both from the perspective of the intelligence community and working in congressional oversight. Could you give your perspective on whether we should reauthorize this provision and whether this permissive presumption approach is workable and preferable?

Ms. SPAULDING. Yes, thank you, Senator. I actually testified a couple weeks ago in the House Judiciary Committee, primarily about the lone wolf provision, and very strongly endorsed that permissive presumption amendment to the lone wolf provision.

I think it addresses what is the real problem, which is—if there is a problem—one of uncertainty about connection to an international terrorist group. As you noted, the lone wolf provision is often referred to as “the Moussaoui fix,” but as an exhaustive study by this Committee demonstrated, there was no need for a fix to FISA to be able to access Mr. Moussaoui’s computer. In fact, the failure to do so reflected a misunderstanding on the part of the Bureau as to the FISA standard. So it is not really necessary to get at the—because the probable cause standard is a relatively low standard, not even “more likely than not,” and because an international terrorist group can consist of two individuals, the ability to meet a probable cause standard that this person is operating with at least one other person is not a very high hurdle.

Having said that, if the Government can make a compelling need, I think the permissive presumption fix is appropriate.

Where I am really troubled is that the provision as now written really reflects I think a cynical—I have expressed it as a Humpty-Dumpty approach to the law, where words mean what I choose them to mean.

Defining someone who is acting entirely alone with no connection to any other person or foreign power as “an agent of a foreign power,” as FISA now does, is a legislative legerdemain that I think threatens to undermine this very important national security tool, and I would take the lone wolf, the true lone wolf, out.

Senator FEINGOLD. Thank you.

Mr. Dempsey, at a hearing on the Select Senate Intelligence Committee a couple weeks ago, Attorney General Gonzales testified that we do not need an ascertainment requirement for roving wiretaps under the FISA as the SAFE Act would mandate because there is no ascertainment requirement for criminal roving wiretaps. Is that correct, and can you respond to what Mr. Collins said about the roving wiretap changes in the SAFE Act, please?

Mr. DEMPSEY. Well, as I read the roving tap authority in Title III, there is an ascertainment requirement. I have to say that in 1998 in an amendment that was made out of scope to the Intelligence Authorization Act, it was watered down, but it is still there. The order is limited to the interception so long as it is reasonable to presume that the person identified in the application was in the reasonable proximity of the instrument to be intercepted. There is a better, I think, roving ascertainment requirement applicable to bugs.

When this Committee, under Senator Leahy and Senator Mathias, first adopted the roving tap authority in 1986, they did have that stronger ascertainment requirement for both taps and bugs. In fact, if you look at the Committee report on the 1986 roving tap provision, they specifically cited terrorism as one of the cases why that was being adopted and why the ascertainment requirement was suited for both taps and bugs of terrorists. And it is still there, albeit in watered-down form for taps. So I have to disagree with the Attorney General on that.

Senator FEINGOLD. Mr. Dempsey, FBI Director Mueller has advocated that we expand the PATRIOT Act as part of the reauthorization process and grant the FBI broad administrative subpoena authority in terrorism cases. He argues that national security letters and Section 215 orders are insufficient to obtain records because apparently they take too long or are too difficult to enforce. How would you respond to Director Mueller on those points?

Mr. DEMPSEY. Well, I think administrative subpoenas is one of the worst ideas that has been around for 30 years, which is how long it has been around for. This is a piece of paper signed by an FBI agent saying, "Give me everything you have," with not even the nominal oversight of a prosecutor that you have with the grand jury subpoena. And in this age of Blackberries and ubiquitous Internet access, I really do not see why, except in the rarest of cases, you would ever need to avoid going to a judge under the minimal showing that is being discussed here to get approval to get papers and records either in a terrorism case or an ordinary criminal case.

Senator FEINGOLD. Mr. Chairman, I thank you for the time. I would just like to ask to place in the record a statement in support of the SAFE Act from Senator Salazar, as well as letters of support from the American Jewish Community and various other outside groups.

Chairman SPECTER. Without objection, they will be made a part of the record.

Thank you very much, Senator Feingold.

Senator Hatch.

Senator HATCH. Mr. Collins, between April 2003 and January 2005, a period of 21 months, delayed search notice warrants were used, I believe, 108 times. Now, in 28 of those cases seriously jeopardizing the investigation was the sole ground for seeking the delay of notice from the issuing court. Now, that is 26 percent of the time. That seems far from catch-all use to me. The words "seriously jeopardize" sound like very narrowing modifiers of the Government's power to request this type of a warrant. I think that most judges would be able to distinguish and determine when circumstances may affect the outcome of a case and when circumstances may seriously jeopardize a case.

These delayed notification warrants have been requested and granted less than one-fifth of one percent of the time, as I understand it. I do not see evidence of abuse here. Am I right on these facts? And where were the cries of injustice when the delayed notice warrants were used in criminal cases before 9/11?

Mr. COLLINS. Senator, you are correct that this was not an innovation of the PATRIOT Act. This was something that existed in

case law and standards had been developed. It was codified in the PATRIOT Act, and the PATRIOT Act specifically gave flexibility to the district judge to set the time limits, and that has really been the primary point of dispute.

I think the other thing that is worth noting about the statistics that, Senator Hatch, you have cited and that the government has supplied in a letter to the Chairman is that the district courts who have reviewed these have, in fact, invoked the flexibility on timing that the PATRIOT Act has granted them. Some have said seven days in particular cases. Another said 10, another said 30. They have, in fact, set it depending in the showing that has been made to them.

Mr. DEMPSEY. Senator, may I comment?

Senator HATCH. Sure.

Mr. DEMPSEY. The catch-all provision, I think, is of concern particularly in relationship to the standard. The standard is reasonable cause—not probable cause, but reasonable cause to believe that the notice may have the adverse effect. So it is almost a double expansion—reasonable cause to believe that it may have an adverse impact.

If you look at those statistics, you see that not a single judge denied a single government request under any prong of the sneak-and-peek test. So in every single case where the government cited serious jeopardy to a case, the court found it and ordered it.

I think that the proponents of this sneak-and-peek provision are in a way trying to have their cake and eat it, too. They say, well, we are just codifying current law. But current law did have as a presumption a 7-day delay period, and yet we have in one case that was referenced by the Justice Department a 406-day delay in notice.

In seven cases, the Justice Department sought unlimited delay. They asked for, and I think in six of the seven or seven of the seven got, delay for the duration of the investigation. I don't think there is a single case on the books prior to this legislation where judges said go on as long as you want.

Senator HATCH. Well, we are talking about terrorists here.

Mr. DEMPSEY. Well, no, we are not.

Senator HATCH. Yes, we are.

Mr. DEMPSEY. Excuse me, Senator, but by and large this has been used in nonterrorism cases.

Senator HATCH. It was used before, too.

Mr. DEMPSEY. They broke into a judge's chambers.

Senator HATCH. Let me take back my time because I want to ask one more question before I finish.

Mr. Collins, it seems to me that the PATRIOT Act takes tools already available to law enforcement in criminal investigations and enables them to use those same tools to go after criminal terrorists. We gave law enforcement the right to do in a terrorism case the same job we would expect them to do in a case against any public menace such as drug dealers, pedophiles, mafia syndicates, et cetera. That is a bright change from the dark past when you weren't allowed to apply these basic tools in the cases of suspected terrorism because of an artificial wall between intelligence and law enforcement.

Is that an accurate assessment? Also, if you have any comments about Mr. Dempsey's comments, I would appreciate those, too.

Mr. COLLINS. I think that one of the goals of the PATRIOT Act was to ensure that there would be counterparts on the intelligence side of the ledger for the tools that are on the criminal side. That doesn't mean that there might not be differences, depending on the circumstances, between those tools, and that is really what the debate comes down to.

Senator HATCH. Okay, and with regard to Mr. Dempsey's comments, if it is justified by the court, I can see why, to protect an investigation, they might grant more than seven days.

Mr. COLLINS. One of the points I made is that the PATRIOT Act was not—when I said it was a codification, I didn't mean it had no change. In fact, I said exactly the opposite in making the point that judges have taken advantage of the flexibility to allow longer times. Somehow, this seven days had gotten into the case law before. That did not go into the statute and they have, in fact, set different time periods in different investigations. The fact that none have been denied may suggest that the government has been quite cautious in its use of it and has made convincing showings that they have not abused it.

Senator HATCH. Yes, I think we ought to presume that rather than to presume the worst.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Hatch.

Senator SESSIONS.

Senator SESSIONS. Thank you, Mr. Chairman. I would just repeat my own evaluation for what it is worth. I was a prosecutor for over 15 years. I issued hundreds and hundreds of subpoena, probably not as many as Mr. Barr did when he and I were U.S. Attorneys together because he had a bigger district to cover, more millions of people. But we issued thousands of them. I was attorney general.

I found nothing in this Act that encroached or really undermined the classical principles of search warrants, nothing that conflicts with fundamental principles of issuing a subpoena. Mr. Barr prosecuted a Republican Congressman. He was appointed by President Reagan in Atlanta, and I saw it in the papers all the time. It was a battle.

I bet you, Bob, you had all of his telephone records, all of his bank records, all of his business records, his calendar diary, notes, phone messages, and you just issued subpoenas for some of that and some you issued search warrants for. Isn't that correct? Isn't that done routinely everyday that a United States Attorney can issue a subpoena for hotel records to see who was in a hotel?

The DEA in a drug case can issue an administrative subpoena for those kinds of hotel and telephone records. Isn't it done everyday all over America?

Mr. BARR. They are done everyday all over America. That really I don't think is the question before the Senate. The question is—

Senator SESSIONS. I don't have but a minute, but I would like in one brief moment, you tell me what is so dangerous about this Act, where we have gone out of historical principles of prosecutorial and investigative authority. You will never convict anybody of bank fraud, Enron or anything else, if you can't get their records.

Mr. BARR. Well, I dare say that the government had plenty of not just reasonable suspicion that crimes were committed in those cases that the Senator cites, but very articulable suspicion. And that is where—

Senator SESSIONS. Very articulable suspicion. Now, what is the standard for issuing a subpoena?

Mr. BARR. An articulable suspicion, I think, is a very sound standard, and we have gotten away from that. That is one of the problems here, Senator, in Section 215 which can be used to reach the exact same records that you and I would not have thought of reaching if we didn't have articulable suspicion.

Senator SESSIONS. Well, if you are brought to trial and there was no basis to obtain the records, you could move to dismiss the indictment if that proof is critical.

Mr. BARR. But you can't do that in a FISA.

Senator SESSIONS. Yes, you can at trial, can you not?

Mr. BARR. Not under Section 215. The person never knows.

Senator SESSIONS. The records they will know.

Mr. BARR. No, they won't. They are in the hands of a third party.

Senator SESSIONS. If you have got their bank records and their bank records are introduced—

Mr. BARR. You would never know if somebody moved under a Section 215 order to get your records because they are not going after your records that you have. They are going after records about you that somebody else has.

Senator SESSIONS. And as we know, counsel, you don't have the classical reasonable expectation of privacy in documents being held by another company. They are that company's documents. What you have in your house, what you have under your control in your wallet, in your pocket—you have an expectation of privacy and that cannot be obtained without a search warrant approved by a Federal judge.

Mr. BARR. I think you do have a legitimate expectation that they will not be gathered and used against you without at least some reason to believe that you have done something wrong, Senator.

Senator SESSIONS. Do you think it is a wrong for a district attorney in a town with 20 motels who has got information that John Jones spent the night in that town to issue a subpoena to every motel there to see if they have a record of John Jones?

Mr. BARR. If there was a reasonable connection with a criminal proceeding or if the government had a reasonable suspicion that he was an agent of a foreign power, yes.

Senator SESSIONS. So this is done all the time. I will let Mr. Dempsey comment.

Mr. DEMPSEY. Yes, Senator, thank you. I think the crucial distinction is that if a prosecutor issued subpoenas to 20 hotels, those hotels could squawk about it. If they thought that subpoena was over-broad, they could squawk about it and that prosecutor would know that at the end of the day his conduct would show up in court, in the light of day, subject to public scrutiny. And if he was casting a fishing net—

Senator SESSIONS. I understand that.

Mr. DEMPSEY. Here, Senator, we are talking about secret intelligence investigations.

Senator SESSIONS. Secret intelligence information, but it involves the security of our country. We have always treated that differently. And, number two, you go to the judge first. The D.A. does not have to go to a judge to issue subpoenas for bank records, medical records, library records. He issues that subpoena and they are produced.

But if he desires to do one involving a terrorist circumstance, he has to go and present the evidence to a Federal court and get court approval before the subpoena is issued, quite different from the other. So, in effect, do you not, Mr. Collins, have court review in advance of the action rather than an opportunity to object at trial later on?

Mr. DEMPSEY. Senator, under 215 there is no factual showing. No facts need be stated by the Government, and it says that the judge shall issue the order, as requested or modified, without naming the target of the investigation and without specifying whose records are sought or what connection they have to that investigation. And the recipient is prohibited forever from telling anybody. He can't complain and that may never show up in court.

Senator SESSIONS. Well, that is very important. If you are conducting a sensitive investigation, Mr. Dempsey—

Mr. DEMPSEY. But that is why—

Senator SESSIONS. Just a second. You have had your comment. If you are doing a sensitive investigation of a terrorist organization and you want to subpoena their bank records, you don't want the banker calling up the terrorist organization and telling them they just subpoenaed your records. This is life and death. It is not academic.

Mr. DEMPSEY. Exactly, Senator, and that is why we should have other protections.

Senator SESSIONS. And it has been done before. You can get court orders today. Before the PATRIOT Act, you could get court orders to direct the recipient of the subpoena not to make it public.

My time is out here, but I just don't—

Chairman SPECTER. This is pretty lively, Senator Sessions.

Senator SESSIONS. Well, I take it very seriously. We are not out of historical traditions of search and seizure on the issue of subpoenas here.

Chairman SPECTER. I was about to offer you a little more time. [Laughter.]

Senator SESSIONS. Thank you, Mr. Chairman.

Mr. Collins?

Mr. COLLINS. If I just may make one point, in addition to having to go to the court first, I think it is notable that the Department in litigation has taken the position that there is a right to challenge a 215 order in court. The Attorney General reiterated that in his April 27th testimony, and that, I think, is one issue that is worth discussing, is what a provision that makes that formal looks like.

The SAFE Act does, in fact, have something there. I think it raises a number of serious questions. I alluded to the fact that it creates an automatic stay and it is not clear to me that there should be an automatic stay right in the statute, as opposed to a

judge determining that it should be stayed pending a resolution of the dispute.

It incorporates the Classified Information Procedure Act which is designed for a criminal context and just carries it over into the civil context without modification. That raises a serious question. It allows these to be filed in any district court in the United States, rather than, as has been the model under FISA, those judges or magistrate judges who have been designated by the Chief Justice and where the facilities are set up to allow this to be done. It creates significant rights of disclosure, again, by analogy to CIPA. All of those, I think, are very serious questions that need careful study if this is going to be articulated, what this review that everyone agrees should be made available would actually look like.

Senator SESSIONS. The pre-issuance review?

Mr. COLLINS. Well, the pre-issuance is the fact that, Senator, as you pointed out, under 215 you can't just pull a piece of paper out of your desk and sign it and get the record. You first have to go to a judge and get an order.

Senator SESSIONS. Well, Mr. Dempsey says you don't have to give any evidence to the judge.

Mr. COLLINS. No. You have to show that there is, in fact, an investigation and that the records—

Senator SESSIONS. Are relevant to the investigation.

Mr. COLLINS. —are relevant.

Senator SESSIONS. That is the standard for subpoenas, isn't it, Mr. Barr, or anybody, prosecutors? It is evidence relevant to the investigation.

Mr. BARR. You have to read the rest of it, Senator—relevant to an investigation to protect against acts of terrorism. That is different from a grand jury standard, much broader.

Chairman SPECTER. Senator Sessions, Senator Leahy has to leave in a few moments. Let's turn to him for a closing comment.

Senator SESSIONS. He issued a lot of subpoenas in his prosecutorial career, also.

Senator LEAHY. I had to go through a judge, I had to go through a judge. I had to go through a judge and I had to show probable cause.

Senator SESSIONS. Not for issuing a subpoena, not probable cause.

Senator LEAHY. For the subpoenas I did—I was a State prosecutor—we had to have probable cause. We had minimal probable cause, but it was there and it was with notice. If not immediately, there was notice and it could then be contested.

Mr. Dempsey, when Senator Hatch cut you off, you were just about to say something about a break-in at a judge's office. What was that all about?

Mr. DEMPSEY. Well, this is one of the sneak-and-peek searches. I mean, I say break-in. It was a sneak-and-peek search under Section 213. The Justice Department has reported on some of the cases in which they have used this authority and a number of them are nonviolent, nonterrorism cases, one a judicial corruption case, clearly a very important matter, but I think that is not what most people thought they were voting for when they voted for the PATRIOT Act.

Senator LEAHY. Let me talk about a few things. Professor Cole, the administration has never used the detention power it requested in Section 412. Does it have any useful purpose or can we just eliminate it?

Mr. COLE. I think it could be eliminated. What we have seen is that without invoking Section 412, the administration subjected over 5,000 foreign nationals to preventive detention using immigration power.

Senator LEAHY. Is that to enhance national security, those 5,000 people?

Mr. COLE. There is absolutely no evidence that it has enhanced our national security. In fact, I think there is considerable evidence that it has undermined our national security. First, as I suggested in my opening remarks, none of the people who were detained and called suspected terrorists by Attorney General Ashcroft repeatedly in the weeks and months after September 11—not one of them stands convicted of a terrorist crime today. So there is no credible evidence of any gain.

The loss from a security perspective is that we have alienated entire communities, Arab and Muslim communities here in the United States, and maybe more importantly Arab and Muslim communities around the world who see us imposing on their nationals burdens and obligations that we would not be willing to bear ourselves.

So, no, I don't think Section 412 is necessary. If the Government can lock up 5,000 people with no connection to terrorism without 412, they clearly don't need Section 412. In fact, what I think is necessary is some congressional legislation that puts restrictions on immigration detention so that it is governed by the same standards that govern criminal detention. Where there is evidence that someone is either a danger to the community or a risk of flight, he or she may be detained, pending proceedings. But without that evidence, no.

Senator LEAHY. I worry that we sometimes feel that if somebody is from anywhere outside our shores, there is going to be a real problem about them. I don't want to call it xenophobia, but it is somewhat creeping, and as the grandson of immigrants it worries me greatly some of the things we are doing that we would never impose, or don't even want other countries to impose on us because, of course, we are Americans and we want to impose it on others.

The debates about closing our borders, and so on—the Senate is going to vote on a supplemental appropriations bill today and it has a substantial increase in immigration provisions which this Committee was never even allowed to look at. It was junk plunked in there, and numerous regulatory changes that I know you have said have impeded the constitutional rights of immigrants.

Should we be looking back at our immigration laws in this country and ask whether maybe we are getting carried away? We are doing so many things that seem out of the mainstream, and I realize it is apples and oranges, but Section 3144, Title 18, so we can lock up witnesses who have information deemed material—I am thinking about Brandon Mayfield, the Portland attorney. My gosh, we got a perfect match on his fingerprints that he was involved in the bombing in Madrid. In fact, he hadn't been there, but we will

just go and seize all his things and ruin his livelihood. He did hang around with Muslims.

The fact that he is out in Portland, Oregon, and the train was in Madrid and we got a false reading on a fingerprint that even under the loose standards of the FBI laboratory shouldn't have gone through—I am getting off the subject. What should we do?

Mr. COLE. I think on the subject of immigration, Senator Leahy, we should be a country that does not permit secret arrests, does not permit secret trials, does not hold people liable for their speech without showing any dangerous conduct, does not deport people for their political associations, and that does not lock people up without some objective evidence shown to a judge that the person needs to be locked up. That is the country we ought to be. That is the country we insist on for citizens.

We ought to extend those same basic protections to the people who live among us who are not citizens. These rights—rights of speech, rights of association, rights of due process—are not privileges of citizenship. They are rights of all persons. They are owned to every human being in the United States and we ought to extend those rights.

I think the Civil Liberties Restoration Act is a great start on that, but as I said before, there has been no hearing on it in either House. I think the supplemental appropriations is definitely a step in the wrong direction going back essentially to the McCarran-Walter Act, where we kept out people like Graham Greene and Gabrielle Garcia Marquez and NATO General Nino Pasti, not for their conduct, but for what they say and for with whom they associate.

Senator LEAHY. Well, Mr. Chairman, I am glad to hear that said because we have to remind ourselves—you know, the Chairman and I have been here about 30 years each and when we first came here, it was at the height of the Cold War, Iron Curtain and all. And I loved going to places behind the Iron Curtain and being able to say to countries with censorship where people would be locked up, whether it was Solzhynitsyn who came to live in Vermont later on, and others, that, boy, in America you can speak out. We protect speech. In fact, what is most important, we protect unpopular speech. It is easy protect popular speech. We protect unpopular speech. I loved being able to say that all over the world as a very distinct hallmark of our democracy and protection of our First Amendment. No other country has the kind of protection that we do. I worry very much about what it does to our image abroad and what it does to us as a people if we pull back from that.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Leahy.

Mr. Dempsey, did you say that Section 213 was used to search a judge's chambers?

Mr. DEMPSEY. Yes, sir. That is reported by the FBI in a letter to Senator Stevens in 2003—excuse me—by the Department of Justice.

Chairman SPECTER. I don't want to conduct a protracted—

Mr. MCCARTHY. Senator, I am sorry. I don't mean to interrupt. My understanding is that that occurred in 1992, like about ten years before the PATRIOT Act.

Chairman SPECTER. Well, I was just about to put into the record a copy of a letter dated May 6 of this year to Senator Roberts, who is Chairman of the Senate Select Committee on Intelligence, concerning testimony that you had provided, Mr. Dempsey, concerning the Department's use of Section 213 of the PATRIOT Act. It is a long letter and we are way over time now, but—

Mr. DEMPSEY. If you could, Senator, could we also place in the record the Justice Department letter in defense of Section 213 that cited that case?

Chairman SPECTER. After I finish my sentence, I will.

I don't intend to go into this in any great detail, but I am going to make this a part of the record, and I am glad to put into the record any document which you think is relevant.

Mr. DEMPSEY. Thank you, sir.

Chairman SPECTER. You don't have to show relevance or cause. [Laughter.]

Chairman SPECTER. We have very generous standards for admitting matters to our record. One of my first exposures to that was Senator Dole one day with a broad, sweeping gesture one day said I am going to clean off my desk and put it all in the congressional Record.

Senator Sessions, do you have any concluding comment?

Senator SESSIONS. I think that is a hint. Mr. Chairman, I was reading, I believe, a book—I gave it to my staff—about 15 years ago, about, I believe, an organized crime case or a big drug case. I think it was an organized crime case. The government used a delayed notification search warrant.

I can't express how important a tool this can be in a big-time case involving a terrorist organization that is seriously threatening our people. It is important in major drug cases, it is important in any big mafia case and cases like that. There are times when you need to be able to determine what is in a residence.

Under normal law, if you want to find out what is in a residence and seize weapons of mass destruction, you go to court. If you have got probable cause, a judge gives you a warrant and you go out and seize the stuff and you take it right back to the police station and you give them an inventory of what you seized. That is the way you do it. In America, it is done probably 5,000 times, 10,000 times a day, everyday, in America.

Under this proposal, it just simply codifies procedures that have been utilized historically by which you provide further evidence that making known to the criminal or the terrorist that you have seized this material can be adverse to the investigation or the public safety. And you have to show this to this court and you can get an order that allows you to not seize the documents that you could actually seize and take back to the police station; just see if they are there, or the chemicals or the bomb material and that kind of thing. This so-called sneak-and-peek has been portrayed as some sort of incredibly intrusive law enforcement technique unprecedented in American history, and it is just not so.

Now, with regard to the issue of subpoenas under FISA, the standard as it comes to me now is whether or not the documents are relevant to an investigation, not whether it provides probable cause or anything like that. Does this motel, hotel, hospital, li-

brary, business, charitable organization have documents relevant to an investigation? And you would normally just issue the subpoena on behalf of the grand jury and they go out and get the documents. I mean, that is the way you do it.

If it is really important and this person can be connected to a terrorist organization or a foreign power, you can go to the FISA court and get a subpoena. You have to get the court's approval first, and then you go out and you get the documents. And he can't reveal that he has been served and he can't quash at that stage.

Now, is it your position, Mr. Collins—and, Mr. Dempsey, I will raise it with you—that if there was some procedure along the way that you could get a quash that that would make you happy? I mean, surely this is not a huge deal.

Mr. DEMPSEY. Well, Senator, first of all I want to say that I agree with you entirely that the risk we face here is grave, that these are extremely serious matters. For that reason, I have said that there is not a single power in the PATRIOT Act that I think needs to sunset; that the records that are at issue here are records that the government should have access to.

I want to engage both at this hearing and afterwards if we have some time in a real dialogue with you to talk about what I perceive as some of the differences between the grand jury subpoena and the 215 order, and where are some of the checks and balances that can ensure that the government has the power it needs, the timeliness it needs, the secrecy it needs.

Senator SESSIONS. Those can be critically important.

Mr. DEMPSEY. Absolutely, but still have some of the checks and balances and oversight. One of the issues that has clearly been put on the table is the after-the-fact challenge or the challenge by the recipient of the order, which is a possible check, an important check.

Often, that person, though, Senator, has very little interest. The records don't pertain to them. As you say, they are business records. And again I worry with this perpetual secrecy and how can we put a little bit more protection at the front end instead of relying on the back-end protection, when the person who has the right to challenge on the back end really doesn't care in many cases and it is almost better for them—

Senator SESSIONS. They don't care at the front end most times.

Mr. DEMPSEY. Well, that is often true.

Senator SESSIONS. But, some, like a bank—a lot of banks now, Mr. Chairman, have a policy that if they are served a subpoena, they notify their customer. That didn't used to be the case.

Mr. DEMPSEY. And I think that is an important possible protection.

Senator SESSIONS. They would prefer a court order saying not to do so. That protects them from being sued by the customer or violating their bank policy.

Chairman SPECTER. Senator Sessions, your second-round time is up, and it is almost noon.

Senator SESSIONS. Thank you for your leadership on this issue.

Mr. DEMPSEY. I hope we can continue the discussion, Senator.

Senator SESSIONS. Thank you very much.

Chairman SPECTER. Mr. Cole, I have one final question for you. If you have a member of Al Qaeda and the only evidence is his membership in Al Qaeda, association with Al Qaeda, but there is no evidence of a terrorist Act and he seeks admission to the United States, there is a grave difficulty in how you protect the country and protect his right of association.

Is there a right of association with Al Qaeda, so that if there is no terrorist act, you would admit him to this country?

Mr. COLE. I think Al Qaeda is a different case, for the following reason. The right that the Supreme Court has announced—

Chairman SPECTER. Well, could you start off by answering my question?

Mr. COLE. I don't think you have the same right of association with Al Qaeda as you would have, for example, with the African national Congress or the Palestinian Authority or the Northern Alliance in Afghanistan, all of which are defined as terrorist groups under the Iraq supplemental appropriation.

Al Qaeda is different because Al Qaeda engages entirely, as far as we can tell, in illegal conduct. That is all they are about. They are not a political organization with a particular agenda which uses some legal means and some illegal means to further that agenda. They are an organization engaged in nothing but illegal conduct.

The standard the Supreme Court identified in the Communist Party cases is when a group engages in both lawful and unlawful activity, it is a violation of the First Amendment principle of free association and a violation of the Fifth Amendment principle of personal guilt to impose liability on an individual by means of his connection to that group without showing some connection to unlawful activities of the group.

Chairman SPECTER. Thank you, Professor Cole.

This has been a very lively and very productive session. It is a surprise to me that all of my colleagues have left already. Oh, no, it is past noon. I can understand why they left.

Thank you, Congressman Barr, Professor Cole, Mr. Collins, Mr. Dempsey, Mr. McCarthy, and Ms. SPAULDING. That concludes our hearing, and we will be pursuing this matter in depth.

Mr. Dempsey, you have all the time you want to find Senator Sessions.

Mr. DEMPSEY. I am going to track him down. Thank you, Senator.

[Whereupon, at 12:01 p.m., the Committee was adjourned.]

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

[Additional material is being retained in the Committee files.]

QUESTIONS AND ANSWERS

Answer to a Question from Senator Biden to Dan Collins
May 10, 2005 Hearing of the Senate Judiciary Committee
on "Continued Oversight of the USA Patriot Act"

Q.: In your written testimony you commented on Section 213's authority to delay notification of the execution of a warrant. Although this section does not sunset, some critics of the PATRIOT Act have alleged that Section 213 does not prescribe any specific temporal limit for the delayed notice to the target(s) of the intercepted communication. This appears to be unique within the federal criminal law section of the U.S. Code, including Titles 18 and 21. While different sections prescribe different temporal limits, all such statutes appear to delimit some outer limit by which, absent good cause shown, the government must notify targets of searches or surveillance. Under 18 U.S.C. 2518(8)(d), for example, the government must notify all individuals whose communications were intercepted under a criminal wiretap "[w]ithin a reasonable time but not later than ninety days" after the conclusion of the wiretap, absent "good cause" shown to the court. (a) Are you aware of any other federal criminal statute, other than section 213, which does not contain a specific time limit? (b) If not, can you tell me why Congress should not impose some reasonable time period, as occurs elsewhere in the Code?

Answer:

Various provisions of the federal criminal code address in different ways the question of when notice of the government's use of an investigative tool must be given.

For example, the statute governing the use of pen registers or trap and trace devices, 18 U.S.C. § 3121, et seq., provides that orders authorizing the installation of such devices shall "be sealed until otherwise ordered by the court." 18 U.S.C. § 3123(d)(1). This non-disclosure obligation is open-ended and applies until affirmatively changed. However, because such devices only capture routing or addressing information as to which there is no reasonable expectation of privacy, see *Smith v. Maryland*, 442 U.S. 735, 742 (1979), the orders governed by § 3123(d)(1) do not implicate searches within the meaning of the Fourth Amendment.

The Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq., dispenses with the statutorily-imposed notice requirement if the government uses a search warrant (as opposed to an administrative subpoena or a court order under the Act) to obtain the contents of a communication that is stored on the system of a "provider of remote computing service." 18 U.S.C. § 2703(b)(1)(A). The extent to which the Fourth Amendment applies of its own force in such a context does not appear to have been squarely addressed by the courts. Cf. *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002) (recognizing the issue, but declining to decide whether "there is a constitutional expectation of privacy in e-mail files").

As you note, Title III, which governs wiretaps, provides that, unless "good cause" is shown on an ex parte basis by the government, notice of a wiretap must be given by the court to

the target "[w]ithin a reasonable time but not later than ninety days" after the "termination of the period of an order or extensions thereof." 18 U.S.C. § 2518(8)(d). The interceptions governed by this statute reach communications that are clearly protected by the Fourth Amendment. See *Katz v. United States*, 389 U.S. 347 (1967).

Under the delayed-notice provisions of Section 213 of the PATRIOT Act — which apply to searches that are governed by the Fourth Amendment — the court shall set the "reasonable period" within which notice of the execution of a search warrant must be given. 18 U.S.C. § 3103a(b)(3). Because, under section 213, the court has the ultimate ability, and the *independent* ability, to supervise and control the length of the delay as appropriate under all of the circumstances, I do not perceive any deficiency in the statute as it now stands and do not believe it needs to be amended.

In particular, there is no reason why Congress should, by statute, adopt a one-size-fits-all approach to the length of delayed notice. Cf. proposed SAFE Act, S. 737, § 3(a)(2) (fixing a firm 7-day initial time limit, subject to 21-day extensions). By contrast, the approach which you suggest, *i.e.*, to amend section 213 so that it follows the notice model of Title III, does not suffer from that defect and, in my view, is not an unreasonable approach. That is, Congress could set a *presumptive* maximum length of the delay, but a longer period could be fixed by the court if the government shows "good cause" why the presumptive maximum period should be exceeded in the circumstances of that case. This might also be combined with authority to seek further extensions as warranted. If this approach were adopted, Congress should not just pick a number out of the air, but should be careful to set the presumptive time period in light of the empirical data about how courts have actually chosen to exercise the discretion currently conferred upon them by section 213.

Ms. Suzanne Spaulding

Question for the record from Senator Patrick Leahy

1. I have long supported modifying the pen register and trap and trace device laws to allow for meaningful judicial review. Under current law, the government need only certify that the information sought is relevant and the judge has no discretion—he must issue the order. I believe that, at a minimum, the government should be required to make a showing that the information sought is relevant, and the judge should make a finding to that effect. Do you agree?

Answer

I agree that pen register and trap and trace laws should provide for meaningful judicial review, as opposed to the current requirement that a judge approve the government's request upon a mere certification without any factual basis. This is particularly important now that the authority includes email communications, which often provide the names of the parties to the communication rather than merely numbers. In addition, special care is required with respect to the use of pen registers and trap and trace devices for domestic intelligence collection, where the scope of authority is far broader than that for a criminal investigation.

The Supreme Court decision that is cited to support a low threshold for approving pen register requests, Smith v. Maryland, 442 US 735 (1979), was handed down in a technological context that is light years from today's. For example, the Court specifically noted the "pen register's limited capabilities," including in its opinion a quote from United States v. New York Tel. Co., 434 US 159, 167 (1977):

Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed....Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.¹

Yet, when pen register authority is used with regard to email communications, the names of the parties are often revealed. Moreover, it is now technologically trivial to match a phone number with a name. And if the legislation recently adopted by the Senate Select Committee on Intelligence becomes law, the pen register provision in Foreign Intelligence Surveillance Act (FISA) will allow the government to demand not only the phone numbers or routing information, but the name, address, all telephone or email usage records, and even credit card or bank account numbers of the target, as well as the name and address of every person with whom they communicate.

Of even greater concern is the way this authority broadened as it migrated from the criminal context into the statutory framework governing the collection of intelligence inside the United States. In order to get an order for a criminal investigation, the government has to certify that the information likely to be obtained "is relevant to an ongoing criminal investigation being

¹ 442 U.S. 735, 742

conducted by that agency." In addition, the order must specify the identity, if known, of the person who is the subject of the criminal investigation. This means there must at least be some known, well-defined criminal activity that forms the basis for the investigation.

However, when Congress gave domestic intelligence collectors the power to order pen registers and trap and trace devices, they required the government to certify only that the information likely to be obtained, with respect to a non-US person, is foreign intelligence information—which is very broadly defined and need not involve any illegal activity—or, with respect to a US person, is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a US person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This latter standard—relevant to an investigation "to protect against" international terrorism—is remarkably broad and, again, need not involve any illegal activity. Moreover, unlike a criminal order, in this intelligence context there is no requirement that the underlying investigation is focused on any particular person(s), or, if it is, that the government indicate their identity. Law abiding citizens who have no knowing connection to terrorist activities but who may have, for example, flown on a flight about which there had been some intelligence "chatter", could suddenly have the government secretly monitoring who they call, who calls them, who they send emails to, who sends emails to them, and what websites they visit.

Moreover, since the statute only provides that the underlying investigation to protect against international terrorism cannot be based solely on first amendment activity (which means it can be based almost entirely on first amendment activity), it would appear that the basis for any particular pen register order that is relevant to that underlying investigation *could be* based solely on first amendment activity.

Intelligence investigations are, by necessity, wide ranging. They are also conducted in secret, without the usual safeguards that have been put in place to protect against abuse in criminal investigations. Therefore, careful oversight becomes absolutely vital.

Requiring the government to provide a judge with some factual basis justifying the request to exercise this authority against an individual, rather than using judges as a rubber stamp anytime a government official provides a certification, will help to ensure some greater degree of oversight over these potentially broad powers.

—Suzanne E. Spaulding

SUBMISSIONS FOR THE RECORD

Campaign for Reader Privacy

American Booksellers Association, American Library Association,
Association of American Publishers, PEN American Center
www.readerprivacy.org

FOR IMMEDIATE RELEASE

For information contact: Oren Teicher (ABA), 800-637-0037, ext. 1267
Larry Siems (PEN), 212-334-1660 ext. 105
Judith Platt (AAP), 202-220-4551
Bernadette Murphy (ALA), 202-628-8410

**BOOK GROUPS HAIL REINTRODUCTION OF
SECURITY AND FREEDOM ENHANCEMENT (SAFE) ACT**

Washington, DC, April 5, 2005 –Organizations representing booksellers, librarians, publishers and writers today welcomed the reintroduction of the Security and Freedom Enhancement (SAFE) Act, promising to mobilize readers and book lovers all over the country to press for passage of the bill, which restores safeguards for reader privacy that were stripped by the USA PATRIOT Act. Senators Larry Craig (R-ID) and Dick Durbin (D-IL) announced the reintroduction of the SAFE Act at a press conference in Washington this afternoon.

The PATRIOT Act's Section 215 amended the Foreign Intelligence Surveillance Act (FISA) to give the FBI vastly expanded authority to search business records, including the records of bookstores and libraries: the FBI may request the records secretly; it is not required to prove that there is "probable cause" to believe the person whose records are being sought has committed a crime; and, the bookseller or librarian who receives an order is prohibited from revealing it to anyone except those whose help is needed to produce the records.

The SAFE Act requires the FBI to have "specific and articulable facts" that show that the person it is targeting is a foreign agent before it may seek a search order from the secret FISA court. The SAFE Act also gives a librarian or bookseller the right to go to court to quash the order; requires the government to show why a gag order is necessary; places a time limit on the gag (which can be extended by the court), and gives a recipient the right to challenge a gag order.

The SAFE Act also limits other powers given to the FBI by the PATRIOT Act, including the power to conduct "roving" wire taps, and to issue National Security Letters, which authorize searches of library computers, and "sneak and peak" search warrants.

"Last year, booksellers, librarians, publishers and writers launched the Campaign for Reader Privacy to restore safeguards for the privacy of bookstore and library records," Oren Teicher, chief operating officer of the American Booksellers Association, said. "We collected nearly 200,000 signatures on petitions in bookstores and libraries, and on our Web site, www.readerprivacy.org, and we are going back to the grassroots this year to collect even more."

ALA Washington Office Executive Director Emily Sheketoff added, "the freedom to read what we choose without the government looking over our shoulder is perhaps the most basic of all the rights guaranteed by the Constitution. In seeking to curb the overly broad provisions of Section 215, we are not trying to thwart government efforts to investigate terrorists. However, we do not believe that the government needs unsupervised, secret powers to learn what ordinary Americans are reading."

Former Congresswoman Pat Schroeder, president and chief executive officer of the Association of American Publishers, said: "Americans understand the need for accurate intelligence to prevent acts of terror, but unless we protect ourselves without sacrificing our freedom, any 'security' we achieve is meaningless. The SAFE Act would restore an important measure of balance to this equation and would keep the government from unwarranted intrusion into the reading habits of ordinary citizens."

Larry Siems, director of the freedom to write program of PEN American Center, emphasized that writers, like all Americans, support strong, targeted laws to confront terrorism and prevent terrorist attacks. But PEN, an international human rights and free expression organization, has documented how, in many countries struggling with real terrorist threats, anti-terror laws exceed their stated purpose. "We have seen time and again how weakening legal protections for individuals may create shortcuts for law enforcement, but that shortcuts inevitably lead to errors and abuses," Siems said.

The SAFE Act, which was first introduced in 2003, is the third bill introduced in the new session of Congress to restore the safeguards for bookstore and library records that were eliminated by the PATRIOT Act. Rep. Bernie Sanders (I-VT) reintroduced the Freedom to Read Protection Act (H.R. 1157) last month. Sen. Russell Feingold (D-WI) reintroduced the Library, Bookseller and Personal Records Privacy Act (S. 317) in February.

Grassroots opposition to the provisions of the PATRIOT Act that undermine civil liberties continues to grow. Five state legislatures and 372 cities and counties across the country have passed resolutions that are critical of the PATRIOT Act. Last week, Montana joined Alaska, Hawaii, Maine and Vermont in passing a resolution. The vote was 87 to 12 in the House and 40 to 10 in the Senate.



The American Jewish Committee

Office of Government and International Affairs

1156 Fifteenth Street, N.W., Washington, D.C. 20005 www.ajc.org 202-785-4200 Fax 202-785-4115 E-mail ogia@ajc.org

May 10, 2005

The Hon. Arlen Specter, Chairman
The Hon. Patrick Leahy, Ranking Member
Senate Judiciary Committee
U.S. Senate
Washington, D.C. 20510

Dear Chairman Specter and Senator Leahy,

I write on behalf of the American Jewish Committee (AJC), the nation's oldest human relations organization with over 150,000 members and supporters represented by 33 chapters nationwide, with respect to today's hearing of the Senate Judiciary Committee on "Continued Oversight of the USA-PATRIOT Act." We respectfully request that this letter be included in the record of the hearing.

AJC commends the Committee for taking up the challenge of evaluating the successes and failures of the PATRIOT Act, legislation whose enactment AJC supported, and that AJC has continued to support, but always with the caveat that it periodically be re-evaluated and adjusted. As all Americans, AJC urgently desires that law enforcement authorities have the tools in hand necessary not only to apprehend those who would commit such heinous acts, but also, to the fullest extent feasible, to prevent such crimes from being committed in the first place. For this and other reasons, AJC hailed passage of the PATRIOT Act in 2001, including provisions that modified then-current surveillance law in recognition of the need to adapt surveillance techniques to make them more relevant to the new technology of the 21st Century. We agree with the Government's assertion that many of the provisions contained in the PATRIOT Act are codifications or natural extensions of prior existing laws. The PATRIOT Act also helped to facilitate what we had long called for, which is a greater capacity for law enforcement to share information among the different agencies in order to avoid duplication of effort, and to achieve more efficient intelligence gathering and analysis.

From the outset, however, we recognized the dangers associated with providing the government these broader powers, particularly because the changes were made on an expedited basis against the background of a horrendous attack on Americans at home. We therefore

The American Jewish Committee
Advancing democracy, pluralism and mutual understanding

May 10, 2005

Page 2

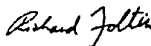
supported inclusion in the USA-PATRIOT Act of sunset provisions to ensure ongoing Congressional oversight and prevent potential abuses of civil liberties. Bearing in mind that our initial support for the PATRIOT Act came with the caveat that its provisions should be re-evaluated in light of further study and the experiences associated with implementation, and given that a number of the Act's provisions are scheduled to sunset at the end of this year, this is an opportune time to consider what types of amendments to the Act are in order.

In light of some three and one-half years' experience since passage of the PATRIOT Act, AJC believes there is indeed room to improve the legislation so as to both enhance our nation's security and protect the civil liberties that help make America the leading defender of democracy and human rights in the world. Last year, AJC endorsed the Security and Freedom Ensured (SAFE) Act, as then framed, as responsible bipartisan legislation that thoughtfully amends provisions of the PATRIOT Act to address civil liberties concerns. At the time, we felt that the SAFE Act placed reasonable limits on the authority given to law enforcement under the PATRIOT Act, without materially hindering their ability to investigate and prevent terrorism.

As you know, the SAFE Act was recently reintroduced in the Senate in revised form. While AJC has not completed its review of the specifics of the revised Senate bill, we support the "mend it, don't end it" approach that the new bill takes, just as did the original measure. The SAFE Act, in both its original form and as revised, represents a commendable effort to balance the need for heightened security and enforcement capabilities with fundamental due process and privacy protections.

In sum, AJC continues to stand by its initial support of the PATRIOT Act as a means to combat the threat of terrorism against our country and its citizens. The time has come, however, to modify certain provisions of the Act so as to more carefully reflect the dual goals of protecting our nation, and its civil liberties. We urge this committee, and Congress as a whole, to seriously consider the changes proposed in the SAFE Act, as potentially an appropriate and balanced means of aligning the PATRIOT Act more closely with these goals.

Respectfully,



Richard T. Foltin
Legislative Director and Counsel

cc: The Honorable Richard Durbin



Office of the Attorney General

Washington, D. C. 20530

October 24, 2003

The Honorable Ted Stevens
 Chairman
 Committee on Appropriations
 United States Senate
 Washington, DC 20510

Dear Mr. Chairman:

The Department of Justice strongly objects to the amendment offered by Representative C.L. ("Butch") Otter and adopted on July 22, 2003 by the House of Representatives, to H.R. 2799, the "Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act of 2004." If it were to become law, the Otter Amendment - which would prohibit the use of appropriated funds to ask a court to delay notice of a search warrant under 18 U.S.C. § 3103a(b) - would seriously hinder the United States' ongoing efforts to detect and prevent terrorism, as well as to combat other serious crimes. The Otter Amendment would prevent federal prosecutors from asking courts to use a judicially created authority that they have used in cases involving organized crime and illegal drugs for many years, indeed, since long before the USA PATRIOT Act. This could result in the intimidation of witnesses, destruction of evidence, flight from prosecution, physical injury, and even death. I urge the Senate to reject any comparable amendment to the counterpart legislation in the Senate and to work to remove the Otter Amendment in conference.

Section 3103a(b) of title 18 of the United States Code, which was added by section 213 of the USA PATRIOT Act, is a vital aspect of the Justice Department's strategy of preventing, detecting and incapacitating suspected terrorists *before* they are able to strike. Section 213 allows *federal judges*, in certain narrow circumstances, to authorize investigators *temporarily* to delay notice that a search warrant has been executed.¹ The law requires such notice to be given

¹ 18 U.S.C. § 3103a(b) provides as follows:

(b) Delay.— With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

within a reasonable period following the execution of the warrant, and such period may only be extended by the court for good cause shown. This codification of pre-existing authority for judicially-approved delayed-notice warrants was enacted when Congress passed the USA PATRIOT Act by overwhelming votes of 357-66 in the House and 98-1 in the Senate.

Although it is a critical tool to the Justice Department's efforts to prevent terrorism, section 213 is hardly an innovation. Quite the contrary, federal courts have had the ability to issue delayed-notice warrants for many years, long before the USA PATRIOT Act. In fact, section 213 is not subject to the USA PATRIOT Act's sunset provision, which Congress reserved for provisions that were regarded as new authorities, specifically because of the long-standing use of delayed-notice warrants. Prior to the USA PATRIOT Act, the law was a mix of inconsistent standards that varied across the country because of differences among federal circuit-court rulings. Section 213 solved this problem by establishing a uniform statutory standard applicable throughout the United States. In other words, the USA PATRIOT Act simply codified a longstanding procedure - delaying notification of a search warrant - which courts had already held is constitutional.

Delayed-notice warrants are an essential tool because there are a number of limited but dangerous circumstances in which providing immediate notification to a suspected terrorist could devastate an ongoing investigation - and even threaten innocent lives. If a suspected terrorist learns contemporaneously that his property has been searched, he may immediately flee the country to escape prosecution. The suspected terrorist would likely destroy computer equipment and anything else containing information about which targets he plans to strike. The suspected terrorist may alert his associates that an investigation is underway, enabling them to go into hiding - or causing them to accelerate their terrorist plot. The suspected terrorist may stop communicating with other members of his cell, preventing law enforcement from learning who else is participating in a plot to kill innocent Americans. The suspected terrorist may close his bank accounts, preventing investigators from discovering who is financing his terrorist activities. And the suspected terrorist may injure - or, even worse, kill - witnesses who have information that could implicate him, and whose cooperation with authorities may be revealed by the search.

In accordance with longstanding law and practice, law enforcement, under the supervision of the federal courts, also needs the continued ability in these cases to protect the integrity of an ongoing investigation - and the safety of the American people - by temporarily delaying when the required notification is given. By law, section 213 can be used only in extremely narrow circumstances - when a federal court determines immediate notification may result in: "*endangering the life or physical safety of an individual*"; "*flight from prosecution*"; "*destruction of or tampering with evidence*"; "*intimidation of potential witnesses*"; or "*otherwise*

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.

seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(a)(2) (emphasis added).

Crucially, in each and every case, section 213 specifically obliges law enforcement to give required notice that a search or seizure has taken place. In fact, *it would be a violation of the USA PATRIOT Act to fail to provide notice.* This provision simply allows investigators, after seeking and receiving a court-issued search warrant, to temporarily delay when the required notification is given. And it goes without saying that no court may issue a search warrant unless there is probable cause. See U.S. CONST. amend. IV ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation").

The notion that the Constitution prohibits delayed-notice search warrants is simply false. The Supreme Court has squarely held that the Fourth Amendment does not require law enforcement to give immediate notice that a search warrant has been executed. In *Dalia v. United States*, 441 U.S. 238 (1979), the Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." *Id.* at 247. In fact, the *Dalia* Court stated that an argument to the contrary was "frivolous." *Id.*

These same types of "delayed-notice" authorities have been on the books for at least 35 years. They are effective, congressionally-enacted, court-approved tools that have helped prosecutors build the cases necessary to lock up Colombian drug lords and the leaders of organized crime. Thirty-five years ago, in Title III of the 1968 Omnibus Crime Control and Safe Streets Act, Congress authorized federal courts to issue temporarily covert wiretap orders. It is precisely because these types of laws *are* constitutional that investigators have for many years been authorized by the courts to install a wiretap in a suspected terrorist's apartment, a spy's car, and a mobster's social club without notifying the suspects.

The lower federal courts have been equally clear in holding that the Fourth Amendment permits law enforcement to give delayed notice that a search warrant has been executed. For example, in *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990), the Second Circuit – in a unanimous opinion by Judge Amalya Kearse – reasoned that:

Certain types of searches or surveillances depend for their success on the absence of premature disclosure. The use of a wiretap, or a 'bug,' or a pen register, or a video camera would likely produce little evidence of wrongdoing if the wrongdoers knew in advance that their conversations or actions would be monitored. When nondisclosure of the authorized search is essential to its success, neither Rule 41 nor the Fourth Amendment prohibits covert entry. ←

Id. at 1336 (emphasis added). In fact, the court emphasized in this drug-trafficking case that delayed-notice searches actually are *less* invasive of privacy than other types of commonly-used investigative techniques:

In devising appropriate safeguards for a covert-entry search for only intangibles, we note that in many ways this is the least intrusive of these three types of searches. It is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. It is less intrusive than a wiretap or video camera surveillance because the physical search is of relatively short duration, focuses the search specifically on the items listed in the warrant, and produces information as of a given moment, whereas the electronic surveillance is ongoing and indiscriminate, gathering in any activities within its mechanical focus.

Id. at 1337; see also *United States v. Ludwig*, 902 F. Supp. 121, 126 (W.D. Tex. 1995) (agreeing that delayed-notice searches "are less intrusive than conventional searches").

The Fourth Circuit, in a child-pornography case, has agreed that nothing in the Fourth Amendment imposes an immediate notification requirement: "the failure of the team executing the warrant to leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment. The Fourth Amendment does not mention notice, and the Supreme Court has stated that the Constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice." *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000). A Second Circuit case likewise confirmed that "[t]he Fourth Amendment does not deal with notice of any kind . . ." *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993).

Before she was elevated to the Second Circuit, District Judge Sonya Sotomayor similarly held that a delayed-notice search was lawful: "The notice requirement of Rule 41(d) has been held by the Second Circuit, however, not to bar covert-entry searches for intangibles - so-called 'sneak and peek' warrants." *United States v. Heatley*, No. S11 96 CR. 515(SS), 1998 WL 691201, at *2 (S.D.N.Y. Sept. 30, 1998).

The Ninth Circuit likewise has recognized that it is appropriate to give delayed notice under certain circumstances. See *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986). In the course of rejecting a search warrant that never required notice to be provided, see *id.* at 1453 ("The warrant contained no notice requirement."), the court explained that searches conducted without contemporaneous notification are appropriate if they are "closely circumscribed," *id.* at 1456. Several years later, in a unanimous opinion authored by Judge Dorothy Nelson, the court held that the Fourth Amendment does not require prior or contemporaneous notification of a search pursuant to a warrant. See *United States v. Johns*, 948 F.2d 599, 605 n.4 (9th Cir. 1991) ("[T]he Fourth Amendment requires that officers provide notice of searches within a reasonable, but short, time after the surreptitious entry.").

Since the USA PATRIOT Act was signed into law on October 26, 2001, the United States has sought, and courts have ordered, a delayed notice warrant under section 213 just 47 times as of April 1, 2003. Yet although this tool is sparingly and judiciously used, it has helped produce some vital successes in the war on terrorism. The following are examples of how court-

issued delayed-notice warrants have been used over the years to fight terrorism and other serious crimes²²:

- Shortly after the 9/11 attacks, a court issued a delayed-notice warrant to search the computer of individuals who were suspected of being affiliated with a terrorist group. The suspects had sent the computer to a shop for repairs, where agents were able to seize the computer and copy the hard drive without immediately notifying the computer owners. If immediate notification had been provided, the individuals would have learned that they were targets of a sensitive anti-terrorism investigation.
- In *United States v. Odeh*, a recent narco-terrorism case, a court issued a section 213 warrant in connection with the search of an envelope that had been mailed to a target of an investigation. The search confirmed that the target was operating a hawala money exchange that was used to funnel money to the Middle East, including to an individual associated with someone accused of being an operative for Islamic Jihad in Israel. The delayed-notice provision allowed investigators to conduct the search without fear of compromising an ongoing wiretap on the target and several of the confederates. The target was later charged and notified of the search warrant.
- In *United States v. Dhafir*, a case in which the defendant is charged with money laundering and a variety of other offenses based on his having sent approximately four million dollars to Iraq in violation of the sanctions, the court issued delayed notification for three searches. The first involved the search of an airmail package that contained a large check bound for an overseas account allegedly used by the target to transfer money into Iraq. A delayed notice warrant also allowed the agents to search and copy the contents of an envelope that the target mailed from Egypt to his office in the U.S. This package contained a ledger showing how the funds had been dispersed in Iraq. A third delayed notification warrant permitted the agents to walk around the target's residence to survey the locks and security system in order to later secretly enter the residence to install the equipment necessary to execute an electronic surveillance order. These warrants prevented the investigation from being jeopardized, and allowed prosecutors to develop critical evidence in the case before the target knew that he was the subject of an investigation.
- In the investigation of an individual who is suspected of possible terrorism and terrorist financing links, the court issued two delayed notice warrants to (1) copy the hard drive of the suspect's computer to determine whether he was communicating with persons overseas and (2) to place an electronic tracking

²² These examples are based on actual cases. Certain facts that are immaterial to understanding how courts have approved delayed-notice warrants have been altered or omitted to protect certain sensitive information that may not be disclosed at this time.

device on his vehicle. The delayed notice warrants allowed other aspects of the investigation to continue, including a lengthy period of surveillance of the suspect's movement with the aid of the tracking device.

- A court issued a delayed-notice warrant to search a box that the FBI received from a cooperating source, who in turn had received the box from a terrorism suspect. The source was not authorized to disclose these materials to the FBI; indeed, it appears that the very reason the suspect gave the box to the source was a concern that government agents executing a search warrant might discover the materials. Contemporaneous disclosure that a warrant was executed could have endangered the life or physical safety of the source who had provided the box to the FBI.
- During the investigation of a domestic terrorist group, agents followed one member of the group to a "safe house." After confirming that the location was indeed a safe house location, court authority was obtained to plant hidden microphones and cameras in the apartment. As a result, the investigators learned that weapons and ammunition were being stored in the safe house. A delayed notice warrant was issued to allow agents to search the apartment and seize the ammunition and weapons. Several cell members were convicted.
- In a narco-terrorism case, the court issued a delayed-notice warrant in the investigation of a New York money laundering organization that was taking pseudo-ephedrine dollars from the Midwest and sending them to individuals with terrorist links in the Middle East. Without the ability to delay notice, the search could not have been conducted without alerting the narco-terrorists to the fact that a large multi-district investigation was underway.
- During an investigation into a drug ring - which may have used its profits to support terrorism - the court granted a delayed-notice search of a business from which money was believed to have been laundered and transferred to the Middle East. Premature disclosure of the search would have jeopardized the safety of an informant, resulted in the destruction of evidence, and alerted numerous targets of the investigation who have yet to be indicted and arrested.
- During a drug investigation, agents had learned about the location of a warehouse through a wiretap. After obtaining sufficient probable cause, a court issued a delayed-notice warrant to search a truck in the warehouse, where agents found 700 kilos of cocaine. Fifteen defendants were indicted, and the main defendants were ultimately convicted and sentenced to life in prison.
- During an investigation into a nationwide organization that distributes marijuana, cocaine and methamphetamine, the court issued a delayed notice warrant to search the residence in which agents seized in excess of 225 kilograms of drugs.

The organization involved relied heavily on the irregular use of cell phones, and usually discontinued the use of cell phones after a seizure of the drugs and drug proceeds, making continued telephone interception difficult. Interceptions after the delayed notice seizure indicated that the suspects thought other drug dealers had stolen their drugs, and none of the telephones intercepted were disposed of, and no one in the organization discontinued their use of telephones.

- In a drug-trafficking case, the court authorized DEA agents to enter a barn and photograph a truckload of marijuana that had been hidden there. Sixteen delayed-notice orders were entered while the agents observed the barn and waited for the defendant to retrieve the drugs, at which time he was arrested.
- When investigating the money laundering aspects of an international drug trafficking operation, it was learned that the suspects were moving money by using false shipping bills on boxes sent through a commercial courier service. The court issued delayed-notice search warrants to intercept two boxes. Agents opened the boxes, examined, counted, and photographed the cash inside, and then repackaged the cash. One of the targets of the investigation was later videotaped accepting delivery of the boxes of bulk cash. The delayed notice warrants allowed the investigation to continue long enough to identify several of the higher-level money brokers.
- A court issued a delayed-notice warrant in the investigation of a heroin-dealing organization. Wiretaps previously had revealed that a large shipment of counterfeit credit cards was about to be made. The delayed-notice warrant allowed agents to copy the credit cards and to notify the credit companies before the cards were sent to the defendants. The delayed-notice warrant allowed the counterfeiting operation to be dismantled while the drug organization wiretaps were preserved.
- In a judicial-corruption case, a court issued a delayed-notice warrant to search the target's judicial chambers and photocopy a "fix book" kept in the desk of the judge's clerk. The book detailed past and future cases which had been fixed or which were to be fixed, and included lists of defendants "to be found guilty." Execution of the warrant resulted in probable cause to set up audio and video surveillance of the chambers. Three court personnel eventually were convicted of mail fraud and civil rights violations.
- In a fraud case, a court issued a delayed-notice warrant to search an office, based on probable cause that \$2.5 million dollars in fraudulent checks were produced on the premises. The order enabled law enforcement to copy the contents of a computer in the office, and examine the data for evidence of the crime, while temporarily maintaining the confidentiality of the warrant.

- During an undercover fraud investigation of a home health agency, the undercover agent learned that the agency was billing for non-rendered nursing services on behalf of approximately 20 subcontractor agencies. A court issued a delayed-notice warrant that allowed agents to enter the business and copy documents that identified the subcontractors, the nurses who purportedly were visiting the patients, and the owners of other home health agencies that were swapping patients with the target agency. The delayed-notice warrant enabled prosecutors to enlarge the scope of the investigation substantially. The investigation led to the indictment of 40 people for various health care fraud offenses.

As these examples demonstrate, judicially approved delayed-notice search warrants can be a critical component of a terrorism or other serious criminal investigation. Such judicially approved search warrants help protect the lives of witnesses and law enforcement officers, preserve valuable evidence, and safeguard important evidence.

In conclusion, the Department of Justice shares Congress's commitment to preserving American liberties while we seek to protect American lives. When testifying before the House Judiciary Committee on September 24, 2001, I stressed: "The fight against terrorism is now the highest priority of the Department of Justice. As we do in each and every law enforcement mission we undertake, we are conducting this effort with a total commitment to protect the rights and privacy of all Americans and the constitutional protections we hold dear." The Department of Justice continues to believe that the USA PATRIOT Act – including section 213 – accomplishes both objectives. This provision reaffirms the courts' ability to protect sensitive information about ongoing domestic and international terrorism investigations for a limited period of time. It simply establishes a uniform statutory standard to guide the exercise of a power that courts have exercised for years and that, like section 213, has never been held to be unconstitutional.

I urge the Senate to reject the Otter Amendment and continue to work in partnership with the Administration in ensuring that America's most vital anti-terror tools remain available to those working every day to detect and prevent catastrophic attacks. If the final version of the bill that is presented to the President includes a provision that forces the courts to allow notice to terrorists and other criminals before a search warrant is executed, I would join the President's other Senior Advisors in recommending that he veto the bill.

377

The Office of Management and Budget has advised that there is no objection to this report from the standpoint of the Administration's program. If we may be of further assistance in this matter, please do not hesitate to contact us.

Sincerely,



John Ashcroft
Attorney General

cc: The Honorable Robert C. Byrd
Ranking Minority Member
Committee on Appropriations

The Honorable Judd Gregg
Chairman, Subcommittee on Commerce,
Justice, State, and the Judiciary
Committee on Appropriations

The Honorable Ernest F. Hollings
Ranking Member, Subcommittee on Commerce,
Justice, State, and the Judiciary
Committee on Appropriations

The Honorable Bill Frist
Majority Leader

The Honorable Tom Daschle
Minority Leader



OFFICE OF BOB BARR
Member of Congress, 1995-2003

**TESTIMONY ON THE USA PATRIOT ACT
BEFORE THE SENATE JUDICIARY COMMITTEE**

**BY
BOB BARR
May 10, 2005**

Chairman Specter, Ranking Member Leahy, distinguished members of the Committee, I am deeply grateful for the chance to testify before the full Committee on this crucial matter.

I believe strongly that the bipartisan support for civil liberties in the aftermath of the tragic 9/11 attacks, support that is so apparent today, will prove the greatest testament to our traditional constitutional values when the history of this era is written. I commend the Committee for playing a lead role in this endeavor.

My name is Bob Barr. From 1995 to 2003, I had the honor to represent Georgia's Seventh District in the United States 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 1970s, I was an official with the Central Intelligence Agency.

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.

Our organization strongly urges 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 arm or agency of government.

To that end, we also urge Congress to improve the Patriot Act by carefully inserting modest checks against abuse. In particular, I urge the Members of the Committee to support the bi-partisan Security and Freedom Enhancement Act (SAFE) of 2005, sponsored by Senators Larry Craig from Idaho and Richard Durbin from Illinois, who both spoke so eloquently earlier in support of the Constitution.

While it would retain every expansion of law enforcement and intelligence authority in the Patriot Act, the SAFE Act would incorporate modest—but essential—new safeguards against abuse.

For the purposes of this hearing, I will focus largely on the SAFE Act's proposed modification to the standard under which FBI intelligence agents may secretly compel the production of personal records using section 215 of the PATRIOT Act, as well the proposed change to the standard for criminal delayed-notification search warrants, known as "sneak and peek" warrants.

First, however, I would like to make clear that, even though I voted for the PATRIOT Act in October 2001, as did many of my colleagues in the House and almost the entire roster of this Committee, I did so with a hesitancy born of 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 anti-terrorism 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 believe now, however, that perhaps my faith was misplaced. The Justice Department has repeatedly disclosed its use and desire to use the

expanded authority in the USA PATRIOT Act in run-of-the-mill criminal cases. Furthermore, the Administration has repeatedly stated its intention to expand the authority in the USA PATRIOT Act, and has floated various pieces of legislation that would do so.

Those of us who support modest changes to the PATRIOT Act seek two things. First, we want Congress to bolster public accountability over the Patriot Act, which would provide greater assurances that the law is serving its intended purpose.

Second, we want to guarantee that extraordinary surveillance powers are being used to keep terrorists at bay, and are not transformed into a general police power that can be used and misused against Americans under the guise of "national security." This concern, is particularly acute among conservatives, who worry about its possible future misapplication of the Patriot Act against pro-life, land rights or Second Amendment activists.

The SAFE Act's proposed changes to section 215 of the USA PATRIOT Act illustrate these dual concerns perfectly. Section 215 of the USA PATRIOT Act amended what was special authority under FISA (the Foreign Intelligence Surveillance Act) to seize rental car, self-storage and airline records for national security investigations.

Prior to the USA PATRIOT Act, the underlying statutes—50 U.S.C. §§ 1861, 1862—applied only to a limited subset of businesses, and it required a showing of "specific and articulable facts" that the individual target was in fact an agent of a foreign power.

Section 215 of the PATRIOT Act removed *both* of these limitations, thereby greatly expanding the power of the government to reach all "tangible things (including books, records, papers, documents and other items)," and lowering the evidentiary standard *below* even that of standard grand jury subpoenas, which are pegged to at least some showing of relevance to *criminal* activities, and which include the additional safeguards of a clear "right to quash" and a right to challenge any secrecy order that may have been imposed on the subpoena.

Some have questioned why the section 215 power has become known as the "library provision," when it does not expressly mention library records and given that it covers so much beyond library records or other

information maintained by libraries. Indeed, many opponents of PATRIOT Act reform point to the fact that library records were not mentioned. PATRIOT Act supporters routinely cite the fact that many people refer to section 215 in this way as evidence of the “hysteria” or “misinformation” among those who seek modest changes to the PATRIOT Act.

This argument is highly disingenuous. In point of fact, library records are not mentioned in the provision, because the provision applies to *much more* than just library records.

Prior to the USA PATRIOT Act, library and bookseller records were not covered by this power, which back 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 any other document, item or record that the government contends is a “tangible thing.”

Section 215 also comes with a sweeping and automatic gag order, without any explicit provision for a recipient to challenge that prior restraint on First Amendment grounds or 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, the power is also unlike 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 presumptively a serious offense.

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 should restore the “specific and articulable facts” requirement for the target of a section 215 order that connects such records to a terrorist, spy or other foreign agent. 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 would -- in addition to restoring the specific and articulable facts standard -- 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 reasonable steps the government has always been able to meet with respect to powers provided under the Foreign Intelligence Surveillance Act 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 if 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.

Before moving on to section 213, I would also point the Committee to the attorney general's recent 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. The number of orders is on the rise.

The second focus of my testimony is 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. This discussion is particularly apt for the Senate Judiciary Committee, as its Members will have the unique opportunity to install additional checks on this overbroad provision. Before discussing our desired reforms to section 213, which is unfortunately not subject to the sunset provision, it may be helpful to take note of some statistics.

On the eve of the April 6th Senate Judiciary Committee hearing, which featured testimony by Attorney General Alberto Gonzales and FBI Director Mueller against changes to the PATRIOT Act, the Justice

Department released statistics on the use to date of section 213 of the PATRIOT Act.

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 five-month difference in timeframe aside, these numbers clearly reveal a substantial increase in use.

Moreover, Chairman Specter also revealed at the April 6th Judiciary Committee hearing 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.

Also, 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. In addition, the statutory language that opens the door to such indefinite delay is directly contrary to the only two appellate court rulings published before the Patriot Act that evaluate secret criminal search warrants with delayed-notification authorized by the lower court.¹ In the first such case, a circuit court held that "in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such a time should not exceed seven days except upon a strong showing of necessity."²

I would also submit that this Committee is in a special position to evaluate sneak and peek warrants. The Judiciary Committee has jurisdiction over the peculiar area of law in which criminal and

¹ Stephen D. Lobaugh, Congress's Response to September 11: Liberty's Protector, *1 Geo. J.L. & Pub. Pol'y* 131, 143 (Winter 2002) (stating, "The Supreme Court has not ruled on the constitutionality of "sneak-and-peek" searches, and only two United States Courts of Appeals have heard such cases.")

² *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

intelligence investigative powers can blur into one another, and where they consequently have to be carefully cabined to protect constitutional rights. I respectfully submit that the sneak and peek statute is one law that is not appropriately cabined, and is currently so broad that it resembles powers associated with foreign intelligence investigations (i.e., *outside* reasonable limitations for criminal powers contained in the Fourth Amendment).

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. 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 rightly 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 Department'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.

Before I conclude, I would also like to discuss an ongoing controversy over a recent federal court decision (currently stayed pending appeal) striking down a provision of the PATRIOT Act as unconstitutional. Though not directly relevant to sections 213 or 215, I suspect it may come up in today's hearing, and I respectfully address it here.

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 so-called "national security letters," or NSLs, for customer records from Internet, telephone and other electronic service providers.

NSLs, as the Committee knows well, are administrative subpoenas issued at the sole discretion of the FBI under a self-certification procedure. They may be used to compel the production of certain types of records held by third-party businesses and institutions. Though the statute held invalid by Judge Marrero only dealt with the types of records mentioned above, other NSL statutes permit their use to obtain financial and credit records.

To be very clear, the Marrero decision struck section 2709 in its entirety, including the amendments to section 2709 made by section 505(a) of the PATRIOT Act. Put another way, 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 amended by section 505(a) with it.³

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 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 inaccurate. 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, analytically speaking, the USA PATRIOT

³ Judge Marrero's decision did not directly 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.

Act is the 800-pound gorilla in the Marrero opinion, and clearly factored into his reasoning.

In sum, then, I would urge the Committee to continue its careful oversight of sections 213, 215 and the rest of the PATRIOT Act, and of thoughtful consideration of amendments like those proposed in the SAFE Act. If we do this right today, if we are able to fix the PATRIOT Act to make it hew to the Constitution while it fortifies our common defense, we will have broken the tragic mold of past national security crises.

Too often in our history, we have acted too quickly in the face of major national security challenges, and have severely deprived our citizens of their God-given rights under the Constitution. Worse, such deprivations have, without exception, been unnecessary to secure our country. In the post-9/11 world, we have strayed perilously close to the edge, and I fear we will fall all the way if the PATRIOT Act is not fixed. If we do, however, meet the test of history and fix the law before it can lead to another historical shame, we will have broken with the past. And we will have done so by securing our liberties and our safety in equal measure. What could be more American than that?

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.



April 5, 2005

The Honorable William Frist, MD
Senate Majority Leader
The Capitol
Washington, DC 20515

Dear Majority Leader Frist:

Today, Senators Larry Craig (R-ID) and Richard Durbin (D-IN) introduced the bipartisan Security and Freedom Ensured (SAFE) Act of 2005. Without question, this legislation will maintain those key Patriot Act powers that provide law enforcement officials with the resources they need to defeat terrorism. In addition, the SAFE Act will modify a few controversial provisions of the law that go beyond this mission and infringe on the rights of law-abiding Americans in ways that raise serious constitutional and practical concerns.

As you know, when Congress passed the Patriot Act just 45 days following the attacks on September 11, 2001, members voted purposefully to ensure that the most extraordinary provisions of the Act be subject to congressional review before expiring in December 2005.

The SAFE Act provides Congress an important opportunity to review and consider amending the few key provisions of the Patriot Act that are out of line with the checks and balances demanded by the Constitution. These include:

- Section 213, which allows government agents to secretly search through people's homes and businesses and seize their personal property without notice for days, weeks, months or perhaps ever.
- Section 215, which allows government agents to collect personal data on law-abiding Americans – such as the books they buy or borrow, their personal medical history, or even records of goods they purchase, such as firearms – without strong evidence connecting the person or their records to the commission of a crime or to a foreign terrorist agent.
- Section 802, which defines terrorism to reach any state or federal crime involving dangerous acts intending to influence the government or citizens.

Patriots to Restore Checks and Balances (PRCB) is a national network of conservatives and civil libertarians whose mission is to ensure congressional review and modification of provisions of the Patriot Act that are out of line with the Constitution and violate



The Honorable William Frist, MD
Page Two

Fourth Amendment freedoms, including the right to privacy. As you know, many Americans have expressed serious reservations about secret searches of their homes and their possessions by federal agents.

PRCB supports the SAFE Act because it will retain the expanded authorities created by the Patriot Act while placing important checks and balances on those authorities. We urge you to co-sponsor this bipartisan bill which will protect the constitutional rights of Americans while preserving the powers that law enforcement needs to combat terrorism.

We have attached a few examples of recent editorials that support congressional review and modification of the Patriot Act to protect Americans' basic freedoms, which the SAFE Act will do.

We hope you will support this important piece of legislation. Now is the time for Congress to review and consider amending these provisions to protect Americans' most fundamental freedoms, and bring the law in-line with the checks and balances demanded by the Constitution.

Sincerely,

Bob Barr
Chair, Patriots to
Restore Checks and Balances

TESTIMONY OF PROFESSOR DAVID COLE BEFORE THE
UNITED STATES SENATE COMMITTEE ON THE JUDICIARY
ON THE USA PATRIOT ACT

May 10, 2005

INTRODUCTION

Thank you for inviting me to testify on the USA PATRIOT Act (hereinafter "Patriot Act"). I am a professor of constitutional law at Georgetown University Law Center, and a volunteer attorney with the Center for Constitutional Rights. The views I express here are my own.

I want to make three points. First, the Patriot Act debate must be understood in context. The debate is fundamentally driven by concerns not only about the four corners of the legislation itself, but by what it reflects about the Bush Administration's approach toward civil liberties in the "war on terrorism." Full Congressional consideration of the concerns expressed around the nation about the Patriot Act, therefore, must not be limited to the sixteen specific sunset provisions, and not even to the Patriot Act itself, but should also consider the impact of executive initiatives outside the Act that have raised serious civil liberties issues. I will first seek to set out these broader concerns as background for the Patriot Act debate, and urge that Congress consider the Patriot Act inquiry the beginning, not the end, of its inquiry into civil liberties in the war on terrorism.

Second, while several of the Patriot Act provisions that are subject to the sunset raise substantial civil liberties concerns, other provisions, not sunsetted, raise even more grave constitutional problems. To my mind, the worst provisions from a civil liberties standpoint are those addressing immigration and material support to "terrorist organizations." I will spend the bulk of my time addressing these provisions, particularly as others on this panel will focus on the sunset provisions.

Third, in my view, of the Patriot Act's sunset provisions, Section 218 raises the most substantial constitutional questions, and calls for significant reforms. That provision is often credited for bringing down "the wall" between foreign intelligence and law enforcement. That

claim is greatly exaggerated. Moreover, Section 218's enactment creates a range of very serious constitutional concerns about the scope of FISA authority and the procedures for introducing FISA evidence in criminal trials that merit sustained Congressional consideration.

I. THE PATRIOT ACT DEBATE IN CONTEXT

Debate about the Patriot Act has been heated almost since its enactment. While only a single Senator, Russell Feingold, voted against it when it was passed just six weeks after 9/11, six states (Alaska, Hawaii, Idaho, Maine, Montana, and Vermont) and over 370 cities and towns have since then enacted resolutions condemning the civil liberties abuses of the Patriot Act and of the Bush Administration's war on terrorism more generally.¹ A bipartisan coalition of liberal and conservative groups has formed an alliance to restore checks and balances,² and a tripartisan caucus has formed in the House with the same goals in mind.³ A bipartisan coalition in the Senate has introduced the SAFE Act, designed to amend many of the surveillance provisions of the Patriot Act.

Defenders of the Patriot Act often lament that in this debate, the Act gets an undeservedly bad rap. It's true that the Act sometimes gets blamed for things with which it has nothing to do. Indeed, many of the worst human rights abuses committed by the Bush Administration in the name of the "war on terror" are not attributable to the Patriot Act – including the pretextual use of immigration law and the material witness law to lock up thousands of Arab and Muslim foreign nationals who had nothing to do with terrorism; the indefinite detention of some persons, including U.S. citizens, as "enemy combatants," without any trial or even hearing; the development and application of computer data mining programs that afford the government ready access to a wealth of private information about all of us without any basis for suspicion; the FBI's monitoring of public meetings and religious services without any basis for suspecting criminal activity under guidelines relaxed by John Ashcroft; and the use of "coercive interrogation" to extract information from suspects in the war on terror, by such tactics as "waterboarding," in which the suspect is made to fear that he is drowning in order to "encourage" him to talk.

¹ For a current list of the resolutions, see the website of the organization that has spearheaded the resolution campaign, www.borde.org. Among the cities that have adopted such resolutions are New York City, Los Angeles, Chicago, Dallas, Detroit, Philadelphia, Washington, DC, Albuquerque, Baltimore, and San Francisco.

² The alliance, Patriots to Restore Checks and Balances, includes the ACLU and such conservative groups as Americans for Tax Reform, Eagle Forum, and the Citizens Committee for the Right to Keep and Bear Arms. See www.checksbalances.org.

³ The Patriot Act Reform Caucus featuring, among others, Congressmen Bernie Sanders (I-VT), Butch Otter (R-ID), and John Conyers (D-MI).

To take just one example, consider the Administration's use of immigration law to embark on a nationwide campaign of ethnic profiling targeting foreign nationals of Arab and Muslim descent. The Administration called in 80,000 men for "special registration," simply because they came from Arab and Muslim countries. The FBI sought to interview 8,000 young men, again simply because they came from Arab and Muslim countries. And the government has admitted to detaining over 5,000 foreign nationals, nearly all of them Arab and Muslim, in anti-terrorism preventive detention initiatives since 9/11.⁴ Many of those detained were initially arrested without any charges at all. They were detained even where the government had no factual basis for believing that they were dangerous or a risk of flight. Men were locked up and designated "of interest" on the basis of such information as a tip that "too many Middle Eastern men" were working at a convenience store. They were held in secret and tried in secret. And in many instances, they were held long after their immigration cases were resolved, simply because the FBI had not yet "cleared" them of connections to terrorism. These measures were putatively designed to identify terrorists.⁵ Yet of the 80,000 registered, 8,000 interviewed, and 5,000 detained, not a single one stands convicted of a terrorist crime to this day.⁶

⁴ On November 5, 2001, the last day the government issued a cumulative total of detainees, the number was 1182. Dan Eggen and Susan Schmidt, Count of Released Detainees Is Hard to Pin Down, *Washington Post*, Nov. 6, 2001, A10 (reporting Justice Department claims that 1182 had been detained to that point). The Department of Homeland Security reports that as of September 30, 2003, another 2,870 persons had been detained pursuant to Special Registration, a program targeted at male foreign nationals from Arab and Muslim countries. U.S. Department of Homeland Security, "Fact Sheet: Changes to the National Security Entry/Exit Registration System," 5. Available at <http://www.ice.gov/graphics/news/factsheets/NSEERSfactsheet120103.pdf>. According to the 9/11 Commission's "Staff Statement No. 10: Threats and Responses in 2001," another 1,139 absconders had been apprehended as of early 2003 under the "Absconder Apprehension Initiative," targeted at aliens from Arab and Muslim countries with outstanding deportation orders (National Commission on Terrorist Attacks Upon the United States, "Staff Statement No. 10: Threats and Responses in 2001," 13; available at http://www.9-11commission.gov/hearings/hearing10/staff_statement_10.pdf). That makes well over 5,000 foreign nationals detained in antiterrorism preventive detention measures.

⁵ For a damning critique of the Administration's use of immigration laws to detain foreign nationals in the wake of September 11, see U.S. Dept of Justice, Office of the Inspector General, *A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks* (April 2003, released June 2003); see also David Cole, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* 17-35 (New Press, 2003).

⁶ Only three of these persons were ever charged with a terrorist crime, all in a

These and many other initiatives undertaken in our name unquestionably constitute abuses of basic liberties – from the right to privacy to the right not to be locked up arbitrarily to the right not to be tortured. But they did not stem from the Patriot Act. The Patriot Act has nonetheless become a symbol for the Administration's disregard for basic civil liberties and constitutional principles because it was the Administration's first salvo in the war on terrorism, and because its approach is emblematic of so much of the Administration's subsequent actions. It infringes constitutional freedoms, discriminates against foreign nationals, and undermines checks and balances on executive power. Moreover, it was adopted, like so many other anti-terrorism initiatives, without sufficient deliberation, and with virtually no attention paid to the costs to liberty and freedom posed by its reforms. As such, it is a fitting symbol for a widespread unease with the Administration's tactics in the war on terror.

The fact that so many civil liberties abuses have arisen outside the Patriot Act does not relieve Congress of its responsibility to investigate these abuses and to provide corrective legislation where appropriate. Congress could, for example, expressly bar the government from inflicting torture and cruel, inhuman, and degrading treatment on any of its detainees anywhere in the world, but it has not. Congress could call for an Independent Commission to investigate the torture scandal, but it has not. Congress could place limits on political spying by the FBI, but it has not. Congress could ensure that data mining programs build in privacy protections, but again it has not. In short, the concerns expressed by many Americans about the Patriot Act go far beyond the literal terms of that document. So, too, should Congress's oversight and inquiry.

"material support to terrorism" trial in Detroit. Two of the three were acquitted on the terrorist charges by the jury. The third was convicted, but his conviction was thrown out in September 2004 after the prosecution admitted that it failed to disclose to the defense evidence that its principal witness had lied on the stand and that its own experts had raised serious doubts about its evidence in the case. See Danny Hakim, "Judge Reverses Convictions in Detroit Terrorism Case," *New York Times*, September 3, 2004, A12.

It is worth comparing judicial and legislative responses to the war on terrorism. The courts have begun to play an important checking role in the war on terror. They have rejected the Bush Administration's assertion that it could lock up anyone anywhere in the world without judicial review.⁷ They have required that the detainees at Guantanamo be provided with access to counsel.⁸ They have invalidated the processes employed by the Combatant Status Review Tribunals and the military tribunals.⁹ They have declared unconstitutional various provisions of the Patriot Act.¹⁰ They have rejected a Justice Department regulation that permitted immigration prosecutors to keep immigrants detained even after immigration judges found no basis for their detention.¹¹ They have ruled that they have jurisdiction to consider a habeas petition from a U.S. citizen held for twenty months without charges in Saudi Arabia allegedly at U.S. behest.¹² They have required the Pentagon, FBI, and CIA to disclose extensive records relating to the torture scandal.¹³ They have declared unconstitutional the government's practice of holding immigration hearings entirely in secret.¹⁴ And they have thrown out terrorism convictions based on prosecutorial misconduct.¹⁵

Never before have courts played such an important checking role in the context of a national security crisis. Perhaps the courts have learned the lesson of excessive deference in World War I, World War II, and the Cold War. Perhaps they have learned the lesson of the importance of checks and balances of the Watergate era. Whatever the reason, the courts have played an increasingly significant checking function.

But the courts are not the only branch with responsibility to uphold the Constitution and

⁷ *Hamdi v. Rumsfeld*, 124 S. Ct. 2633 (2004); *Rasul v. United States*, 124 S. Ct. 2686 (2004).

⁸ *Al Odah v. Bush*, 346 F. Supp. 2d 1 (D.D.C. 2004).

⁹ *Hamdan v. Rumsfeld*, 344 F. Supp.2d 152 (D.D.C. 2004). *In re Guantanamo Detainee Cases*, 355 F. Supp. 2d 443 (D.D.C., 2005)

¹⁰ *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Humanitarian Law Project v. Ashcroft*, 309 F. Supp. 2d 1185 (C.D. Cal. 2004).

¹¹ *Ashley v. Ridge*, 288 F. Supp. 2d 662 (D.N.J. 2003).

¹² *Abu Ali v. Rumsfeld*, 350 F. Supp.2d 28 (D.D.C. 2004).

¹³ *ACLU v. Department of Defense*, 339 F. Supp. 2d 501 (S.D.N.Y. 2004).

¹⁴ *Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002); *but see North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198 (3rd Cir. 2002).

¹⁵ *See supra* note 6.

to check aggrandizing behavior by the Executive. Congress shares that responsibility. With a few exceptions, Congress has not played that role in the current crisis. The Patriot Act debate is a welcome start, but it should be only the beginning.

II. IMMIGRATION AND MATERIAL SUPPORT

Much of the Patriot Act is uncontroversial from a civil liberties perspective. Provisions increasing resources for patrolling the northern border, strengthening money laundering laws, eliminating some barriers to information sharing between law enforcement and intelligence officials, and improving visa processing, raise few concerns. But many provisions of the Patriot Act are deeply troubling from a civil liberties standpoint. And in many instances, the reforms they introduce have not been shown to have made us safer. I will focus my remarks on the immigration and material support provisions, because these provisions simultaneously raise the most significant constitutional concerns and have received the least attention.

A. Immigration Provisions

The immigration provisions of the Patriot Act, Sections 411 and 412, authorize exclusion of foreign nationals for speech, deportation for innocent associations with disfavored groups, and detention without charges. They go far beyond any legitimate need to protect the nation from terrorist threats. And they infringe on basic rights of speech, association, and due process. Yet Congress has not taken up these concerns, and is poised to make the problems far worse in a little-noticed part of the Iraq supplemental appropriations bill approved by the House on May 5, 2005, and slated for a vote in the Senate this week.

1. Deportation for Associations

Section 411 of the Patriot Act allows the government to expel foreign nationals – even long-time lawful permanent residents – based solely on their association with a disfavored organization. The Act permits deportation for “material support” to any organization blacklisted as “terrorist” by the Secretary of State or the Attorney General. It is no defense to show that one’s support to the group furthered only lawful, nonviolent ends, nor is it any defense to show that the group has not engaged in any terrorist activities. If this law had been on the books in the 1980s, any foreign national who donated to the African National Congress for its largely lawful, nonviolent opposition to apartheid in South Africa would have been deportable, because the State Department designated the African National Congress a terrorist group until it came to power in South Africa with the fall of apartheid.

The reach of the Patriot Act deportation provisions is illustrated by a current case I am handling for the Center for Constitutional Rights. It involves Khader Hamide and Michel Shehadeh, two Palestinians in Los Angeles who have lived here as lawful permanent residents for more than thirty years each. They have never been charged with a crime. Yet the government is seeking their deportation under the Patriot Act, passed in 2001, for conduct they engaged in

nearly two decades earlier, in the 1980s. The government alleges that they are deportable under the Patriot Act for having distributed magazines of a Palestine Liberation Organization faction, and for having raised money for humanitarian aid to Palestinians in the West Bank and Lebanon. On the government's view, it does not matter that these activities were lawful at the time they were engaged in, or that they are protected by the First Amendment.

A second case that illustrates how far-reaching this provision is involves the deportation of an Indian man.¹⁶ In that case, the court held that the Patriot Act authorized the man's deportation for having set up a tent for religious services and food, simply because some unidentified members of a designated terrorist organization reportedly came to the services and partook of the food. There was no showing that the Indian man intended to further any terrorist activity by setting up the tent. Such deportations do not make the United States safer.

2. Ideological Exclusion

Section 411 is even more expansive with regard to the grounds for denying foreign nationals entry in the first place. It resurrects the practice of "ideological exclusion," keeping people out of the country not for their past or current conduct, not even based on any reasonable concern that they might engage in criminal or terrorist conduct once here, but based solely on their speech. If they say something that the Secretary of State considers to "endorse terrorism," they may be kept out. In 2004, the Bush Administration apparently invoked this provision in denying a visa to Tariq Ramadan, a highly respected Swiss scholar of Islam who had been offered a chair at Notre Dame.

3. Preventive Detention Without Charges

Section 412 of the Patriot Act allows the Attorney General to lock up foreign nationals without charges for seven days, and indefinitely thereafter if they are charged with an immigration violation. The law does not require any showing that the foreign national poses a danger to the community or a risk of flight – the only two constitutionally valid reasons for preventive detention. And it permits the Attorney General to keep the foreign national locked up even after he has been granted relief from removal, which is akin to saying that the government can keep a prisoner behind bars even after the governor has granted him a pardon. The government has not yet invoked this provision, calling into question its claim that the authority was absolutely essential to fight terrorism.

4. The REAL ID Act and the Revival of McCarran-Walter

Congress has done nothing to address these problems. Indeed, it has not even held a hearing on the many immigration abuses that have been perpetrated in the name of the war on terrorism since 9/11. And it is about to enact still broader exclusion and deportation grounds as

¹⁶ *Singh-Kaur v. Ashcroft*, 385 F.3d 293 (3d Cir. 2004).

part of the Iraq supplemental appropriations bill. The REAL ID portion of that bill includes little-discussed provisions that dramatically expand the grounds for deportation and exclusion, and for all practical purposes revive the McCarran-Walter Act approach, in which foreign nationals, even permanent residents, can be deported for speech, associations, and conduct that would clearly be constitutionally protected if engaged in by U.S. citizens.

Under the REAL ID provisions, foreign nationals will be deportable for membership in or support of any so-called "terrorist organization." I say "so-called" because the Act defines terrorist organization so broadly that it includes any group of two or more individuals that has ever used or threatened to use a weapon against person or property (except for mere personal monetary gain). The organization need not ever have been designated as "terrorist" by anyone, so long as it used or threatened to use a weapon. Under this definition, the Israeli military, the Northern Alliance, the African National Congress, the Irish Republican Army, the Nicaraguan Contras, the Palestine Authority, and many militant anti-Castro Cuban groups would be "terrorist organizations," even though none has been so designated by the Secretary of State.

The REAL ID Act then makes it a deportable offense to be a member of such a group, to "endorse" such a group through speech, or to provide such a group with any "material support." The provisions are retroactive, so people can be deported today for speech and associations lawfully engaged in years ago. And its punishment extends even to children, who may be expelled simply for having a parent who advocated a disfavored idea.

Under this law, an immigrant whose mother supported the African National Congress's lawful, nonviolent antiapartheid work during the 1980s would be deportable today, as would an immigrant who supported the Northern Alliance, the Israeli military, or the Palestinian Authority. DHS will argue that it is no defense to say that one's support had no connection to the group's violent activities, nor to point out that the United States itself has supported and continues to support many such organizations. Indeed, in the very same appropriations bill that includes this law, Congress has appropriated \$5 million to assist the Palestinian Authority with an audit.

Fifteen years ago, Congress repealed the then-infamous McCarran-Walter Act. Each time that law had been invoked to bar a writer (Carlos Fuentes, Gabriel Garcia Marquez), a politician (Ireland's Gerry Adams, Nicaragua's Tomas Borge), a scholar (Belgian economist Ernst Mandel), or a NATO general (Italy's Nino Pasti), the government's actions were roundly condemned. We exported the notion that the free exchange of ideas was critical to a healthy democracy, but simultaneously barred unpopular ideas and politics at the door. In 1990, Congress laid that history to rest by repealing the McCarran-Walter Act and affirming that we were a strong enough country to tolerate ideas with which we disagreed.

We are now on the verge of reviving the McCarran-Walter Act in the name of the war on terrorism. None of these measures is necessary to protect the United States. Even before the Patriot Act, the government could deny entry to and deport any foreign national involved in terrorist activity, or who supported terrorist activity in any way. What it could not do was

exclude and deport for speech, associations, and activities that do *not* further terrorism. But there is little reason to believe that these provisions have made us safer. Does it really make us safer to keep out a world-renowned scholar of Islam? Or to deport two men for distributing magazines in the 1980s?

B. Criminal Material Support Provisions

The Patriot Act also expanded the most expansive “anti-terrorism” criminal law on the books prior to its passage – 18 U.S.C. §2339B, which criminalizes the provision of “material support” to designated “terrorist organizations.” The Patriot Act expanded this already expansive law by criminalizing pure speech. It amended the criminal ban on material support to designated terrorist organizations by banning “expert advice or assistance” – without regard to what the advice consists of. In a case that I am handling for the Center for Constitutional Rights, a federal court declared this Patriot Act provision unconstitutional.¹⁷ In that case, I represent a human rights organization that seeks to provide human rights training to a Kurdish organization in Turkey that has been designated a “terrorist organization.” The government has argued that it may criminalize as “expert advice” this human rights organization’s advice on human rights advocacy, without regard to the fact that the advice was being offered to encourage the group to pursue peaceful means to resolve its disputes and to *discourage* resort to violence. The court held the provision unconstitutionally vague.

In the first prosecution brought under this provision, the government argued that a student at the University of Idaho should be found guilty for operating a website that featured links to other websites that in turn included speeches preaching violent jihad. It was irrelevant, the government contended, that there was no evidence that the student himself had advocated any violence. An Idaho jury acquitted the student on all terrorism charges.

Congress amended the ban on “expert advice or assistance” in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004) (“Intelligence Reform Act”). But the amendment fails to resolve the constitutional problem with the ban. The federal court declared the ban unconstitutionally vague, so Congress added a definition. But the definition unfortunately only makes the term more ambiguous. It defines “expert advice or assistance” as “advice or assistance derived from scientific, technical or other specialized knowledge.” 18 U.S.C. §2339A(b)(3). Given that “expert advice” would on its own terms already seem to imply some sort of specialized knowledge, it is difficult to see how the Intelligence Reform Act clarifies the provision in any meaningful sense.

¹⁷ *Humanitarian Law Project v. Ashcroft*, 309 F.Supp.2d 1185 (C.D. Cal. 2004).

Other amendments in the Intelligence Reform Act are equally problematic. Federal courts in the *Humanitarian Law Project* case had also held unconstitutionally vague the bans on providing "training" and "personnel" to designated terrorist organizations,¹⁸ and Congress sought to add definitions of these terms as well. But as with "expert advice or assistance," the definitions provide little if any clarity. The Intelligence Reform Act limits "training" to "instruction or teaching designed to impart a specific skill, as opposed to general knowledge." 18 U.S.C. §2339A(b)(2). But this does not clarify the law. Indeed, when the government previously proposed that the statute be interpreted to include that precise limitation, the Ninth Circuit unanimously rejected the argument that it would save the statute: "The government insists that the term is best understood to forbid the imparting of skills to foreign terrorist organizations through training. Yet presumably, this definition would encompass teaching international law to members of designated organizations."¹⁹

The statute may be even more vague now, for it requires individuals to attempt to guess at whether their instruction involves a "specific skill" or "general knowledge." Is human rights advocacy or peacemaking a specific skill, or general knowledge? Is driving a car "general knowledge" or a "specific skill"? What about training in lobbying Congress, speaking to the public, or engaging in public advocacy in the press?

At oral argument before the en banc Ninth Circuit in *Humanitarian Law Project*, the government's attorney, Douglas Letter, was asked specifically to apply this new definition to a number of hypotheticals. In that colloquy, Mr. Letter maintained that teaching English would constitute a forbidden "specific skill," that teaching geography would be permissible because it constitutes "general knowledge," but that teaching the political geography of terrorist organizations would constitute a "specific skill." Letter's response only underscores the hopeless ambiguity created by the new distinction. What if a course on geography included within it a section on the political geography of terrorist organizations? What if it included a section on the history of geography, or the geography of a specific region? Would these be impermissible "specific skills," or permissible parts of "general knowledge?" The new definition provides no more guidance on these questions than the previous prohibition on "training." Thus, the new prohibition on "training" falls for the same reasons that the old did.²⁰

Congress's definition of "personnel" also offers little precision. The new definition of "personnel" draws a distinction between acting under the organization's "direction and control," which is prohibited "personnel," and acting "entirely independently" in support of a group, which

¹⁸ *Humanitarian Law Project v. Reno*, 205 F.3d 1130 (9th Cir. 2000).

¹⁹ *Humanitarian Law Project*, 205 F.3d at 1138.

²⁰ Shortly after the Intelligence Reform Act was signed into law, the Ninth Circuit remanded the *Humanitarian Law Project* case to district court for consideration in light of the amendments. *Humanitarian Law Project v. United States DOJ*, 393 F.3d 902 (2004).

is permitted. But that distinction does not solve the problem. Advocating for a designated group by writing an op-ed opposing its designation or arguing that the material support statute is unconstitutional is clearly protected speech. Yet under the statute, it would be permissible only if undertaken "independently," and not if done under the group's "direction and control." Would running the op-ed by the group's leader for approval, or discussing its themes with him, constitute acceptance of "direction," or would that be "independent"?

What about a lawyer providing her legal services to a group in connection with its challenge to a designation? A lawyer could generally be said to be acting under the "direction" of her client, as, subject only to professional obligations, a client's wishes are determinative. When this issue arose in litigation involving the lawyer Lynne Stewart, the government argued that "personnel" meant "under direction and control." Attempting to apply that concept, the government's lawyer opined that a lawyer acting as "house counsel" would be acting impermissibly under the organization's "direction and control," but an outside counsel doing the same work would be seen as "independent." *United States v. Sattar*, 272 F.Supp.2d 348, 359 (S.D.N.Y. 2003). The court in *Sattar* held the "personnel" ban unconstitutionally vague. *Id.*

Finally, the Intelligence Reform Act expanded the material support ban by adding a new bar on the provision of any "services," a term not further defined in the law. That term is at least as broad as "expert ... assistance" or "personnel," both of which have already been held unconstitutionally vague. Thus, Congress added another unconstitutionally vague term to a statute already found to be shot through with such provisions.

The deeper problem with the material support statute, at least as interpreted by the government, is that it imposes liability on individuals without requiring any proof that they intended to further any terrorist or violent act. According to the government, one who provides human rights training to a designated organization is guilty even if it is undisputed that human rights training cannot be used to further terrorism, and even if it is undisputed that the human rights training actually had the intent *and* effect of reducing the recipient group's resort to violence. Under this law, one who worked with terrorist organizations for the sole purpose of teaching them Mahatma Gandhi's principles of nonviolence in order to dissuade them from violence would nonetheless be criminally liable as a terrorist.

That approach violates both First and Fifth Amendment principles. The Supreme Court long ago held that one has a right to support a group that engages in both legal and illegal activities, and that the government may not prosecute one for his connection to such a group absent proof of specific intent to further the group's illegal activities.

In *Scales v. United States*, 367 U.S. 203 (1961), the Supreme Court held that the First Amendment right of association and the Fifth Amendment requirement of personal guilt precludes the imposition of vicarious criminal liability based on an individual's "status or conduct" in connection with a group, unless the government also shows that the individual specifically intended to further the group's illegal activities. The Court wrote:

In our jurisprudence guilt is personal, and when the imposition of punishment on a status or on conduct can only be justified by reference to the relationship of that status or conduct to other conceded criminal activity (here advocacy of violent overthrow), that relationship must be sufficiently substantial to satisfy the concept of personal guilt in order to withstand attack under the Due Process Clause of the Fifth Amendment.

Scales, 367 U.S. at 224.

The Ninth Circuit in *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 133-34 (9th Cir. 2000), held that the statute's general ban on material support satisfies the First Amendment because it penalizes not membership itself, but material support.²¹ But the *Humanitarian Law Project* court's distinction between material support and membership is intellectually untenable, as it would render the right of association a meaningless formality. The right to be a member of a group without the right to support the group in any way – by dues payments, donations, or even volunteering one's services – would be a worthless fiction. Groups literally cannot exist without the material support of their members. If the *HLP* court's rationale were correct, Congress could have evaded all the Supreme Court decisions barring imposition of guilt for membership in the Communist Party simply by criminalizing the payment of dues or provision of services to the Party. Indeed, on the *HLP* court's reasoning, a law selectively prohibiting all donations to the Green Party would be constitutional so long as individuals retained an entirely symbolic "right" to join the Party.

In the real world, there is no meaningful distinction between a prohibition on membership and a sweeping prohibition on material support. Both have the impermissible effect of barring any conduct in association with the proscribed group. Nor is there any meaningful distinction in judicial doctrine. The Supreme Court in *Scales* expressly stated that penalizing "conduct" on the basis of its connection to a proscribed group was unconstitutional absent a specific intent showing, 367 U.S. at 224, and the Supreme Court and lower courts have repeatedly recognized that "contributing money is an act of political association that is protected by the First Amendment." *Service Employees Int'l Union v. Fair Political Practices Comm'n*, 955 F.2d 1312, 1316 (9th Cir.), cert. denied, 505 U.S. 1230 (1992).

C Administrative Material Support Provisions

Section 106 of the Patriot Act amends an administrative scheme that has also been used to target "material support" of organizations and individuals deemed "terrorist." This provision authorizes the government to freeze assets of domestic corporations and individuals without showing any violation of law, and without any meaningful adversarial testing of its basis for

²¹ The court did not address the Fifth Amendment due process principle of personal guilt.

doing so. It allows the government to freeze all assets of any individual or entity simply by declaring that it is "under investigation" for violating an economic embargo on providing goods or services to a designated "terrorist." The government has placed such embargoes on dozens of organizations and hundreds of individuals, all around the world. The government claims that the authority to designate stems from the International Emergency Economic Powers Act, which never mentions the word "terrorist." There is no statutory or even regulatory definition of a "terrorist" for purposes of IEPEA, and therefore a terrorist is whatever the Administration says it is.

Section 106 permits the Treasury Department to freeze all assets of a U.S. citizen or corporation merely by stating that they are "under investigation" for having a financial transaction with such an embargoed entity. The provision then allows the Treasury Department to defend its actions in court by submitting secret evidence that the challenger cannot see or rebut. This authority has been used to freeze the assets of several of the largest Muslim charities in the United States. When the charities have sued in federal court to challenge their designation, they have been met with secret evidence.²² Moreover, given that there is no statutory or regulatory definition of a designated "terrorist" under IEPEA, it is entirely unclear what standard courts are to apply in assessing whether a designation is appropriate. This law gives the Executive branch a wide-ranging blank check to freeze the assets of any entity or person it chooses, under a literally standardless authority, and then to defend its actions in secret. It is possible that some or all of the half-dozen or so charities that the government has targeted were guilty of funneling money to further terrorism. But it is also possible that all of the charities are entirely innocent. We cannot know, because the Patriot Act eliminated any fair process for distinguishing the innocent from the guilty.

There is no question that funding terrorist activity should be prohibited. It was prohibited long before the Patriot Act. What the criminal and administrative provisions added by the Patriot Act do is extend government sanctions – including substantial prison sentences – to conduct that is *not* intended to further terrorist activity, and that in fact does *not* further terrorist activity. In addition, the Treasury Department provisions deprive those targeted of any fair opportunity to show that their actions had nothing to do with terrorism. In the name of cutting off funds for terrorism, then, these provisions criminalize speech and deny citizens basic due process rights.

III. SECTION 218 AND "THE WALL"

Of the surveillance provisions that are subject to sunset, to my mind the most constitutionally dubious may be Section 218. That provision substantially expanded authority to conduct wiretaps and searches under the Foreign Intelligence Surveillance Act (FISA) without probable cause of criminal activity. The number of FISA searches has dramatically increased since the Patriot Act was passed, and for the first time now exceeds the number of wiretaps

²² *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156 (D.C. Cir., 2003); *Global Relief Found., Inc. v. O'Neill*, 315 F.3d 748 (7th Cir., 2002).

issued on probable cause of criminal activity. Yet because of the secrecy that surrounds FISA searches, we know virtually nothing about them. The target of a FISA search is never notified that he was searched, unless evidence from the search is subsequently used in a criminal prosecution. Even then the defendant cannot see the application for the search, and therefore cannot meaningfully test its legality in court. And while the Attorney General is required to file an extensive report on his use of criminal wiretaps, listing the legal basis for each wiretap, its duration, and whether it resulted in a criminal charge or conviction, no such information is required under FISA. The annual report detailing use of the criminal wiretap authority exceeds 100 pages; the report on the use of FISA is a one-page letter.

Section 218 of the Patriot Act expanded the reach of FISA searches and wiretaps by allowing their use even where the government's primary purpose for investigating is criminal law enforcement. Prior to the Patriot Act, where the government's primary focus was criminal law enforcement, it was required to satisfy the criminal probable cause standards set forth by the Fourth Amendment of the Constitution. It had to show probable cause that the target of the search had evidence of crime in his possession, or had committed a crime. Where, by contrast, the government's principal purpose was not criminal law enforcement but foreign intelligence gathering, it could obtain a warrant for a search or wiretap under FISA simply by showing that the target was an "agent of a foreign power." That term is loosely defined to include any employee of any political organization made up of a majority of noncitizens. The warrant application need not show probable cause of criminal activity. Thus, literally applied, FISA would authorize a search or wiretap of a British lawyer working for Amnesty International, without any requirement of suspicion that the lawyer be engaged in illegal activity.

The Patriot Act extended that loose standard to investigations undertaken primarily for criminal law enforcement purposes, so long as "a significant purpose" of the search is also foreign intelligence gathering. A secret court upheld this amendment in a secret one-sided appeal by the government soon after the Patriot Act was enacted.²³

Defenders of this provision often claim that it eliminated a "wall" between criminal law enforcement and foreign intelligence agencies. But that is an exaggeration. FISA did not require such a wall before the Patriot Act was enacted. It did not bar prosecutors or law enforcement agents from turning over information to intelligence agents, nor did it stop foreign intelligence agents from sharing with criminal prosecutors evidence of crime that they had discovered in their investigations, whether under FISA or otherwise. Evidence obtained in FISA searches could be, and was, used in criminal trials long before the Patriot Act.

There were unquestionably many barriers to information sharing before 9/11. But their principal source was not FISA, but administrative and bureaucratic culture. Agencies were engaged in turf wars, and there were few if any mechanisms or incentives in place to break down the institutional boundaries between agencies. Legitimate concerns about not revealing sources

²³ *In re Sealed Case No. 02-001*, 310 F.3d 717 (For. Int. Surv. Court of Review 2002).

make information sharing difficult even in the most well organized operations. But the blame for these problems cannot be laid at the foot of FISA.

Critics of the wall sometimes suggest that before the Patriot Act, once a foreign intelligence investigation became primarily a criminal investigation, the government would have to take down the tap. But that is also not true. Once an investigation became primarily criminal in nature, government agents would simply have to satisfy the standards applicable to criminal investigations – namely, by showing that they had probable cause that the tap would reveal evidence of criminal conduct. The tap or the search could then continue. If an investigation has become primarily criminal in nature, it should not be too much to ask that the government show probable cause of criminal conduct to carry out a search or wiretap.

Indeed, the Constitution demands no less. FISA's constitutionality turns on an untested assumption that the government may engage in searches and wiretaps for foreign intelligence purposes on a lower showing of suspicion than is required for criminal law investigations. FISA does not require the government to show probable cause that evidence of a crime will be found, but only probable cause that the target of the search is an "agent of a foreign power." "Foreign power" is in turn defined so broadly that it encompasses any political organization comprised of a majority of noncitizens. Where "U.S. persons" are the target of a FISA search, the government must make additional showings, but to search the home of a foreign national here on a work permit, for example, the government need only show that he's an employee of an organization made up principally of noncitizens. It need not show that the individual be engaged in any criminal wrongdoing whatsoever, much less terrorism.

If FISA searches are constitutional, then, they must be justified on the basis of some application of the "administrative search" exception to the general Fourth Amendment rule requiring probable cause and a warrant for criminal law enforcement searches. That exception permits searches in limited settings on less than probable cause where the search serves some special need beyond criminal law enforcement. The FISA Court of Review relied on precisely this exception to find FISA searches valid. But the Supreme Court has carefully limited the "administrative search" exception to situations in which the government is pursuing a special need divorced from criminal law enforcement – e.g., highway or railroad safety, secondary school discipline, or enforcement of an administrative regime. It has refused to apply the exception where the government is engaged in criminal law enforcement, as in a checkpoint to search for cars carrying drugs. And the Court has also refused to apply the exception where the government has a "special need," but is using criminal law enforcement to further that need. Thus, it struck down a hospital program that subjected pregnant mothers to drug tests for the ultimate purpose of protecting the health of the fetus, where the hospital shared the test results with prosecutors in order to threaten the mothers with criminal prosecution if they did not seek drug treatment.

Where an investigation becomes primarily focused on criminal law enforcement, therefore, the "administrative search" exception no longer applies, and Supreme Court doctrine

would compel the government to meet the traditional standards of criminal probable cause. Before the Patriot Act, FISA conformed to that requirement. By abandoning that distinction and allowing searches on less than probable cause where the government is primarily seeking criminal prosecution, Section 218 raises a serious constitutional question. Thus, Section 218 was not only unnecessary to bring down the wall, but may render FISA unconstitutional.

Two reforms short of repeal are worth considering. First, if Section 218 is to be retained, thereby expanding the scope of FISA searches, Congress should revisit FISA's definition of "agent of a foreign power" and "foreign intelligence information." Those terms, particularly as applied to non-U.S. persons, are sweeping, and have *nothing to do with terrorism*. As noted above, the definitions are so broad that they would authorize a tap of a British lawyer for Amnesty International, to gather any information that might relate to foreign affairs. It is one thing to claim that FISA authorities should be available to investigate terrorism; it is another matter entirely to extend those same powers to persons engaged in no criminal activity whatsoever. Thus, the definitions of "agent of foreign power" and "foreign intelligence information" should be narrowed.

Finally, Section 218 and other reforms have made it increasingly likely that information obtained through FISA wiretaps and searches will be used against defendants in criminal cases. In light of these developments, a useful reform at this point would be a provision permitting criminal defendants – or their cleared counsel – an opportunity to review the initial application for the FISA wiretap or search when contesting the admissibility of evidence obtained through a FISA search. Under current law, they have no such opportunity. Without access to the warrant application, defendants and their attorneys cannot meaningfully challenge the legality of the tap or search in the first place. And when government officials know that their actions will never see the light of day, they are more likely to be tempted to cut corners. An amendment requiring disclosure of FISA applications where evidence is sought to be used in a criminal trial would encourage adherence to the law by putting federal officials on notice that at some point the legality of the FISA warrant would be subjected to adversarial testing. Concerns about confidentiality could be met by limiting access to cleared counsel where necessary, and/or by applying the protections of the Classified Information Procedures Act. But there is no good reason for the current blanket exemption against the production of all such applications in criminal cases. The presumption should be in favor of adversarial testing where evidence is to be used in a criminal case.

CONCLUSION

In its treatment of foreign nationals, its expansive definition of "material support" to terrorist groups, and its authorization of surveillance not tied to probable cause of criminal activity, the Patriot Act has substantially eroded fundamental constitutional freedoms. It did so in the name of fighting terrorism, but many of its authorities are written far more broadly than that motive would warrant – penalizing speech and association, eliminating fair procedures for distinguishing the guilty from the innocent, and authorizing searches without probable cause and

secrecy without compelling justification. Measures more carefully tailored to terrorist activity might well have been justified. But the last thing the Patriot Act could ever be accused of is careful tailoring

Testimony of Daniel P. Collins
before the Senate Committee on the Judiciary
May 10, 2005

Chairman Specter, Senator Leahy, 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, some 16 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. In my view, these 16 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 some of the specific PATRIOT Act provisions that are up for "sunset" review, 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 law enforcement 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 placed upon the use of a particular tool. I have previously outlined some of these principles in my prior testimony before this Committee, and I think it is useful to summarize them again here:

- *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 respect 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. 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 criminals with new ways to thwart legitimate and legally authorized law enforcement action. Cyberspace must not be permitted to become a “safe haven” for criminal activity. 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 16 pertinent sections of the PATRIOT Act properly enhance the abilities of law enforcement in a manner that respects and preserves our freedoms.

(1)-(2) Sections 201 and 202

Title III — the wiretap statute — sets forth a number of stringent requirements that must be met before a court may issue an order authorizing a wiretap. One of the requirements is that the investigation must involve an offense that is on Title III’s list of offenses that are eligible for wiretapping. 18 U.S.C. § 2516. The Patriot Act modestly expands this list — which already includes a variety of serious offenses such as money laundering and bank fraud — to include six terrorism offenses, unlawful possession of chemical weapons, and computer fraud and abuse.

Pub. L. No. 107-56, §§ 201, 202, 115 Stat. at 278. In adding these offenses to the list of those eligible to be investigated by wiretapping, the Act leaves unchanged the full panoply of substantive protections provided by Title III. Moreover, the notion that there is a rational and defensible privacy interest in precluding wiretapping to investigate *terrorism* — while permitting it to be used to investigate, say, bribery in sports contests — is very difficult to defend. Sections 201 and 202 are a straightforward application of the principle that law enforcement should have at least the same tools to fight terrorism that it has to fight organized crime.

(3)-(4) 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."

(5) 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 any substantial reason why this provision should not be made permanent.

(6) 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.

Against this backdrop, the amendment that would be made by Section 2 of the SAFE Act, S. 737, seems quite significant. Section 2 appears to be clear in saying that, to avoid the advance specification requirement for “facilities and places,” it is *not* enough to have a detailed “description of the target”; one must know “the *identity* of the target” (emphasis added). What this means is that, even though the Government could describe in great detail a particular agent of a foreign power of whom they are aware, if they can not identify the person, then FISA surveillance must be limited to only those physical facilities that can be specified in advance. Moreover, this would remain true even though the Government could show (as it is required by Section 105(a)(3)(B) to show) that there is 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 the target. The marginal effect of Section 2 would thus appear to be that, even though a “John Doe” foreign agent can be shown regularly to engage in the practice of moving from one disposable cell phone to another, the Government could not be authorized to continue to stay with him unless each

such facility had been specified in advance in the order. It is hard to discern why such a rule would be desirable.

The apparent intent of Section 2 of the SAFE Act is to make the roving wiretap provisions of FISA parallel to those for ordinary criminal roving wiretaps in Title III. Under 18 U.S.C. § 2518(11), the requirement in § 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 whether the "identification" requirement thus imposed by Title III is identical to that envisioned by Section 2 of the SAFE Act, the apparent intent of Section 2 is to 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 Section 2 overlooks a crucial difference between § 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 SAFE Act Section 2's 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 Section 2 would be to make FISA roving wiretaps *harder* to obtain than Title III wiretaps.

(7) 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 permits 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(c)(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.

(8) Section 209

Section 209 of the PATRIOT Act eliminates the anomalous disparity in prior law between the standards for obtaining stored email and those for obtaining stored voicemail. Under prior law, voicemail stored with a third party required a full-blown Title III order, but stored email (and voicemail on the criminal's home answering machine) could be obtained with a regular search warrant. From a technological-neutrality perspective, this did not make a lot of sense. The PATRIOT Act amends the law so that a search warrant will do in such cases. Pub. L. No. 107-56, § 209, 115 Stat. at 283. Because a stored voicemail is, by definition, not a live communication but is instead a record of a completed communication, the more stringent regime created by Title III for contemporaneous interception of communications is unwarranted here. A search warrant, with its requirement of a probable cause finding by a neutral magistrate, should be sufficient.

(9) Section 212

Section 212 of the PATRIOT Act provides a defined authority for electronic communications service providers to make voluntary disclosures of customer records or communications. Specifically, Section 212 permits voluntary disclosure of the *contents* of communications in certain emergency situations and also codifies the various circumstances in

which an ISP may disclose customer records *other* than the contents of a communication. See Pub. L. No. 107-56, § 212(a)(1)(D), (E), 115 Stat. at 284-85.

Notably, the authority given by Section 212 to disclose the content of communications in emergency situations was repealed, and re-enacted in a different form, by the Homeland Security Act. See Pub. L. No. 107-296, § 225(d)(1), 116 Stat. 2135, 2157 (2002). As such, that authority is no longer subject to the PATRIOT Act's sunset provision. Allowing Section 212 to expire would thus sunset the authority to make certain voluntary disclosures of *records* (including disclosures of records in an emergency), thus creating the anomalous result that an ISP, in an emergency, could disclose the *contents* of communications, but not the less-sensitive customer *records* of the subscriber associated with those communications. This does not make a great deal of sense. Moreover, the additional situations (other than an emergency) in which Section 212 permits voluntary disclosures of customer records (*e.g.*, when already authorized by 18 U.S.C. § 2703; when the subscriber consents; when necessary to protect the ISP's network and other rights; and when made to another non-governmental entity) do not seem unreasonable. This provision should be made permanent. (I would note, parenthetically, that the voluntary disclosure authority in 18 U.S.C. § 2702(c)(5), which was added by the PROTECT Act, is permanent and would not be affected by a sunset of Section 212.)

(10) 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?

(11) 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).

Despite what some of its critics seem to imply, this narrowly drafted business records provision 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 does *not* authorize federal agents to rummage through the library records of ordinary citizens. Moreover, it would make no sense to create a 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 4 of the SAFE Act would amend the FISA so that the authority conferred by Section 215 could only be exercised if “there are 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. Would Section 4 bar the agents from getting those records for all 5 persons? It would seem so. Under Section 4, it must be shown that "the person to whom the records pertain" is an agent of a foreign power, i.e., that the *individual* whose records are sought is a foreign agent. 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), Section 4 would seemingly require more. 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).

(12) Section 217

Section 217 of the PATRIOT Act eliminates the loophole in prior law under which *hackers* were arguably protected by the wiretap law from law-enforcement monitoring authorized by the operators of the computers they invade. Pub. L. No. 107-56, § 217, 115 Stat. at 290-91. Section 217 contains appropriately drawn language that permits such monitoring only with the authorization of the owner or operator of the "protected computer" that has been hacked, and it requires that the monitoring be conducted in such a way as to ensure that it "does not acquire communications other than those transmitted to or from the computer trespasser." *Id.*, § 217(2), 115 Stat. at 291. This sensible provision should be retained.

(13) 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.

(14) Section 220

Section 220 properly recognizes the inherently interstate nature of electronic communications by allowing nationwide service of search warrants for electronic evidence. Pub. L. No. 107-56, § 220, 115 Stat. at 291-92. No real advantage would be gained by allowing this provision to lapse. It did not change the substantive standards under which judges issue such warrants, and the change is logistically efficient, especially in a time-sensitive situation, and it

reduces the disproportionate burdens that would otherwise fall on those districts which contain major ISPs (such as the Northern District of California and the Eastern District of Virginia).

This provision should be made permanent.

(15) Section 223

Section 223 provides for civil liability for certain unauthorized disclosures of intercepted communications. Pub. L. No. 107-56, § 223, 115 Stat. at 293-95. This is a pro-privacy provision that, happily, has not yet had occasion to be invoked. I can think of no substantial reason why it should not be made permanent.

(16) 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.

Section 213

Although it is not subject to the PATRIOT Act's sunset provision, I would also like to say a few words about Section 213 of the PATRIOT Act, because it has been the subject of much attention and discussion.

Section 213 of the Patriot Act codifies long-standing authority to delay notification of the execution of a warrant. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990). It does so with proper safeguards: the court must independently find "reasonable cause" to justify the delay; the court must set forth in the warrant the "reasonable period" for such delayed

notice; and such a deadline may be extended only upon a subsequent finding by the court that "good cause" has been shown for the additional delay. 18 U.S.C. § 3103a(b). These stringent safeguards are entirely appropriate, but they are also entirely adequate. Although the revisions that would be made by Section 3 of the SAFE Act in S. 737 are not as extensive as those that were contained in the prior version of the SAFE Act in the 108th Congress (S. 1709), I continue to believe that the changes made by Section 3 would be a mistake. In particular, there is no substantial reason why delayed notice should not be authorized when notification could result in the jeopardizing of an entire ongoing investigation. So long as the court has the ultimate ability, and the *independent* ability, to supervise and control the delay, and the length of the delay, immediate notification should not be required when such serious concerns are present. Moreover, there is no persuasive reason why applications for renewals of such orders must be personally reviewed by the Attorney General, the Deputy Attorney General, or the Associate Attorney General.

* * *

I would like to make one final point. Some have criticized that many of the PATRIOT Act's reforms are not specifically limited so as to apply only in terrorism cases. Once again, I think this criticism reflects a failure to appreciate what sensible policy in this area entails. For example, if the principle of technological neutrality makes general sense, there is no reason why it should be limited to terrorism cases. Is it a rational privacy policy to say that persons committing *bank fraud* should have a leg up over law enforcement if they use one communications technology rather than another? The fact that terrorism concerns motivated the effort to fix the problem in this area does not mean that the problem should not be fixed in a comprehensive and rational manner.

425

In closing, the PATRIOT Act is an invaluable and landmark piece of legislation that has worked to protect American lives while preserving American liberties. The 16 provisions that are currently subject to sunset should all be made permanent.

I would be pleased to answer any questions the Committee might have on this subject.

- 20 -

EFF Section 215-1036

**Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology¹**

**before the
Senate Committee on the Judiciary**

May 10, 2005

Mr. Chairman, Sen. Leahy, Members of the Committee, thank you for the opportunity to testify at this important hearing. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

In CDT's view, there are few if any provisions in the PATRIOT Act that are per se unreasonable. In CDT's view, there is not a single kind of record or communication covered by the PATRIOT Act to which the government should be denied access. 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, every provision of the PATRIOT Act that is of concern can be fixed, preserving the investigative tool, but subjecting it to appropriate standards and judicial and legislative oversight.

In order to understand what is right and what is wrong with the PATRIOT Act, consider the key protections that traditionally surround government access to private information under the Fourth Amendment:

- First, as a general rule, searches and seizures and access to private data should be subject to prior judicial approval.
- Second, a warrant or subpoena must describe with particularity the items to be seized or disclosed.
- Third, individuals should have notice when the government acquires their private data, either before, during or after the search.
- Finally, if the government overreaches or acts in bad faith, there should be consequences, including making sure the government does not use anything improperly seized.

These components of a Fourth Amendment search -- judicial approval, particularity, notice and consequences for bad faith behavior -- are independent. When it is necessary to create an exception to one, that does justify creating a blanket exception from all four. However, too often in the PATRIOT Act, when the government had a good argument for dispensing with

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.

one or another of these protections, it insisted that Congress eliminate all of them. Too many of the powers in the PATRIOT Act lack any of the traditional checks and balances. Take for example, Section 215, the business records provision:

- The judicial approval is not serious – the judge is presented with no factual basis for the request and has no discretion to turn it down.
- The particularity standard of “agent of a foreign power” was eliminated and replaced with no particularity at all.
- Unless the target is actually charged with a crime and the records are used against him at trial, he is never notified that his records have been disclosed to the government.
- The government faces no consequences for overreaching, particularly since the innocent person whose records are disclosed never knows of it.
- There is no public reporting on the use of the technique and even the classified reporting to Congress seems to have been slow in coming and unsatisfactory when it arrived.

The question to be asked as we move forward is, “Recognizing that there is sometimes a need for secrecy, or sometimes no time to get a warrant, what would be wrong with restoring or strengthening the other checks and balances applicable to traditional searches and seizures?”

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.

Intelligence Investigations Are Different From Criminal Investigations – Their Broader Scope and Greater Secrecy Call for Compensating Controls

One of the Justice Department's central themes in defending the PATRIOT Act changes is that the Act's standard of mere relevance to an intelligence investigation is the same as the standard for grand jury subpoenas in criminal cases. A simple answer to this is that, if the government wanted to use a grand jury subpoena, it could without the PATRIOT Act, since international terrorism is a crime.

On a more sophisticated level, it is necessary to recognize the differences between foreign intelligence investigations and criminal investigations. These differences are so fundamental that they require different standards, and in some cases stricter controls, for intelligence investigations.

- First, the scope of intelligence investigations is broader than criminal investigations. Intelligence investigations cover both legal and illegal activities. Intelligence investigations of US citizens can be opened in part on the basis of First Amendment activities; intelligence investigations of non-citizens can be opened purely on the basis of protected speech; and in either case, once opened, intelligence investigations can involve extensive monitoring of political activities and lawful associational activities. In criminal investigations, the criminal code provides an outer boundary, and a prosecutor is often involved to guide and control the investigation. Foreign intelligence investigations can gather information about persons without any suspicion of involvement in criminal activity.
- Second, 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. In the case of a grand jury subpoena, the government is bound by secrecy, while the recipient can publicly complain and the target is often given a letter telling him he is the target; in the case of a disclosure order in a national security case, the recipient is bound by secrecy and the target normally never knows that he is being investigated.
- Third, criminal investigations are focused on obtaining evidence for use at trial. An intelligence investigation is driven not by a desire to arrest and convict, but by a range of foreign policy interests. In the ordinary criminal case, information can be used only at trial. Information obtained by grand jury subpoena, except as permitted by the PATRIOT Act, cannot be disclosed to anyone except a law enforcement officer and cannot be used for any other purpose than law enforcement. The breadth of disclosure of intelligence information is very broad, including intelligence, military, diplomacy,

policy development, protective, immigration, and law enforcement. The "big show" for criminal investigations is the trial, where defendants are entitled to the full panoply of Constitutional protections. At trial, the government's conduct is open to public scrutiny and the defendant can appeal an unfavorable decision.

For all of these reasons, the analogy to subpoena standards is inapt. The government is given different powers in intelligence investigations than it has in criminal investigations. Different powers require different standards. The PATRIOT Act failed to include protections that respond to the differences between intelligence investigations and criminal investigations and provide appropriate protection of Fourth Amendment principles. 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.

-- **Judicial approval, 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 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 intelligence investigation of al Qaeda (or UBL) and that investigation will go on for the foreseeable future. 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 eliminated, and all record demands should be brought under an enhanced Section 215 (with an appropriate exception for emergency circumstances). 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, surveillances 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 email, 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 reexamined, 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 proponents of Section 213 rarely mention that, 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 non-violent 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 or sneak and peek searches. 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 email 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 "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 seven 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 seven 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 anti-terrorism 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 seven 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 investigation 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 seven 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 seven days was an appropriate time period. Indeed, DOJ’s internal guidance recognizes that seven days is the most common period, but also suggests that it may seek much longer delays. Congress should set a basic seven day rule, while permitting the Justice Department to obtain additional seven-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. In Section 505 of the PATRIOT Act similarly expanded the government's power to obtain telephone and email 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. Secondly, 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:

- o Seizure of assets (Sec. 806)
- o Disclosure of educational records (Secs. 507 and 508)
- o 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 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 seven 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 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 show to 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 important 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.

For more information, contact:
Jim Dempsey
(202) 637-9800 x112
<http://www.cdt.org>



LEAGUE OF WOMEN VOTERS®
OF THE UNITED STATES

President
Kay J. Maxwell
Greenwich, Connecticut

April 4, 2005

Vice-Presidents
Linda Claire McDaniel
St. Louis, Missouri

Mariys Robertson
Boulder, Colorado

Secretary-Treasurer
Shirley Eberly
Rochester, New York

Directors
Sarah Diefeudorf
San Francisco, California

Jan Flapan
Chicago, Illinois

Jane Gross
Plantation, Florida

Xandra Kayden
Los Angeles, California

Odetta MacLeish-White
Gainesville, Florida

Carolle Mullan
Lubbock, Texas

Carol Reimers
Hingham, Massachusetts

Olivia Thorne
Wallingford, Pennsylvania

Mary Wilson
Albuquerque, New Mexico

Executive Director
Nancy E. Tate

The Honorable Larry E. Craig
The Honorable Richard J. Durbin
United States Senate
Washington, D.C. 20510

Dear Senators Craig and Durbin:

The League of Women Voters of the United States is pleased to endorse the Security and Freedom Enhancement (SAFE) Act of 2005. We greatly appreciate your leadership in introducing this legislation that addresses some of the most problematic provisions of the USA PATRIOT Act.

For the past 84 years, members of the League have been steadfast in their conviction that the need to protect against security threats to America must be balanced with the need to preserve the very liberties that are the foundation of this country. There are fundamental principles that guard our liberty – from independent judicial review of law enforcement actions to prohibitions on indiscriminate searches – that must be preserved.

By placing limits on “sneak and peek” searches and “John Doe” roving wiretaps and requiring increased public recording of the use of the Foreign Intelligence Surveillance Act, the SAFE Act would provide reasonable checks on some of the most extreme sections of the USA PATRIOT Act.

The League of Women Voters believes that the SAFE Act would preserve broad authority for law enforcement officials to combat terrorism. At the same time, it would protect innocent Americans from unrestricted government surveillance. We look forward to working with you to pass the SAFE Act.

Sincerely yours,

Kay J. Maxwell
President

1730 M STREET, N.W., SUITE 1000, WASHINGTON, DC 20036-4508
202-429-1965 Fax 202-429-0854
Internet: <http://www.lwv.org> E-mail: lwv@lwv.org

Statement
United States Senate Committee on the Judiciary
Continued Oversight of the USA PATRIOT Act
May 10, 2005

The Honorable Patrick Leahy
United States Senator, Vermont

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, COMMITTEE ON THE JUDICIARY
HEARING ON CONTINUED OVERSIGHT OF THE USA PATRIOT ACT
MAY 10, 2005

Today's hearing continues this Committee's oversight and review of the USA PATRIOT Act. We heard from Attorney General Gonzales and FBI Director Mueller at our hearing on April 5th. We heard further from the Department of Justice at a classified briefing on April 12th. This morning, we will hear from several non-government witnesses about their views of the PATRIOT Act.

It is interesting to note that our counterparts in the other body are also holding another hearing this morning on the PATRIOT Act. In addition, the Senate Select Committee on Intelligence has held a series of hearings on the PATRIOT Act. All told, the enhanced surveillance provisions of the PATRIOT Act have been the focus of more than a dozen hearings this year alone, and more during the last Congress.

It is no mystery why the Republican-controlled Congress, which has all but abdicated its oversight responsibilities in many other areas, has devoted so much attention to the PATRIOT Act. In the final negotiating session on the PATRIOT Act, former House Majority Leader Dick Armey and I insisted on adding a sunset provisions for certain governmental powers that have great potential to affect the civil liberties of the American people. These sunset conditions are the reason we are here today. It is the reason our colleagues on other committees are revisiting the PATRIOT Act. And it explains why we are finally getting some answers from the Department of Justice, although the fact that Chairman Specter takes his oversight responsibilities as seriously as he does has also helped a great deal.

The PATRIOT Act is not a perfect piece of legislation, if such a thing even exists. I said as much when we passed it, just six weeks after the 9/11 attacks. In negotiations with the Administration, I did my best to strike a reasonable balance between the urgent need to address the threat of terrorism, and the need to protect our constitutional freedoms. I was able to add many checks and balances that were absent from the Administration's draft, along with provisions to address such other concerns as border security and the FBI's translator problem. Other members of this Committee and in Congress were able to include improvements as well. I made clear that congressional oversight would be especially important for these new government powers. I always knew, and noted at the time, that we in Congress would have to revisit these issues when the immediate crisis, and the emotional aftermath of the crisis, had receded a bit.

As we all know, the vast majority of the provisions of the PATRIOT Act are not subject to sunset. Of the handful that will expire at the end of the year, some are non-controversial and can be renewed with little or no modification. Others require greater scrutiny.

At our hearing in April, Attorney General Gonzales said he was open to any ideas that may be offered for improving these provisions. This was a refreshing departure from the combative stance of his predecessor, who spent hundreds of thousands of dollars of taxpayer money on a public relations

campaign to stem criticism of the PATRIOT Act. Now, with the impending sunset less than eight months away, we need to move beyond the positioning rhetoric and focus on what really matters for the country and for the American people.

Legitimate concerns have been raised about various powers granted by the PATRIOT Act, not so much for how they have been used, but for how they could be used, and for cloak of secrecy under which they operate. Since September 11th, Americans have been asked to accept restrictions on their liberties; they deserve to know what they are getting in return. Until then, this Senator will not ask the American people to give up anything more.

Many of us on the Committee have been working on ways to improve the PATRIOT Act, and a number of proposals are already on the table. For example, Senator Durbin, Senator Craig, and Senator Feingold have proposed corrective legislation, and I commend them for their leadership and hard work.

One thing that I hope we can all agree upon is the need to clarify the procedures for compelling the production of records from third parties in terrorism and intelligence investigations. Last September, Judge Victor Marrero in the Southern District of New York enjoined the FBI from issuing certain "national security letters," both because they bar or substantially deter judicial review, and because their permanent ban on disclosure operates as a prior restraint on speech in violation of the First Amendment.

The invalidated provision first passed Congress nearly 20 years ago, as part of the Electronic Communications Privacy Act, or ECPA. I was proud to be the primary Senate sponsor of that law, although the national security letter provision was added by a Republican member of the Intelligence Committee. Since then the provision has been amended, or relevant definitions within it have been amended, at least three times since 1986 -- most drastically by the PATRIOT Act. It was only after these amendments to the law that Judge Marrero raised issues about its expanded use by the FBI and the Department of Justice. These are legitimate issues, in my view, but whatever we may think of Judge Marrero's decision, we need to address it promptly, before the constitutional defects he identified jeopardize the FBI's anti-terrorism mission. At the same time, it may make sense to require approval at the highest levels of the Department before a national security demand may be made for certain highly confidential materials such as library, bookseller, and medical records.

I also hope we can reach consensus to modify section 206 of the PATRIOT Act, which authorized the use of "roving wiretaps" in foreign intelligence investigations. I supported the inclusion of this authority in the PATRIOT Act in order to bring FISA into line with criminal procedures. As I said at the time, "This is the kind of change that has a compelling justification, because it recognizes the ease with which targets of investigations can evade surveillance by changing phones." In fact, the original roving wiretap authority for use in criminal investigations was enacted as part of ECPA. But while the need for roving wiretap authority is undisputed, the language of section 206, as amended by later legislation, is troubling in its ambiguity and clearly could be improved.

Much has been written about the pen register provisions of the PATRIOT Act. Long before September 11, 2001, I supported modifying the pen register and trap and trace device laws in three respects: first, to give nationwide effect to pen register and trap and trace orders; second, to clarify that such orders can cover computer transmissions and not just telephone lines; and third, to update the judicial review procedure which, unlike any other area in criminal procedure, bars the exercise of judicial discretion in reviewing the justification for the order. The PATRIOT Act modified the pen register and trap and trace laws in the first two respects, but did not allow for meaningful judicial

review. The impending sunset of section 214 of the PATRIOT Act gives us another opportunity to consider this essential guard against abuse.

These are just some of the matters before us as we revisit the PATRIOT Act. We will also hear today from David Cole, an authority on the immigration provisions that were included in the PATRIOT Act. It is regrettable that at the same time our committee is conducting this careful review of the PATRIOT Act, the Republican conferees on the supplemental appropriations bill agreed to include the REAL ID Act's expansion of the terrorism-related grounds for inadmissibility and deportability that we negotiated in the PATRIOT Act. This committee never had the opportunity to consider those expansions, and none of the Democratic conferees on the supplemental bill were even included in conference negotiations.

Earlier this year, we celebrated the first National Sunshine Week with a hearing on open government and bipartisan calls for responsiveness and accountability. We should carry that theme into this process of oversight and legislating.

The sunset provisions of the PATRIOT Act ensured that we would revisit that law and shine some sunlight on how it has been implemented. Dick Arney and I were afraid that the Administration would not tell the American people what was going on, as it turned out, we were right.

I believe that many of us would consider reauthorizing the expiring PATRIOT Act powers, with some modifications, but there must be mechanisms in place to guarantee that the government remains accountable for the use of those powers. Judicial review, public reporting, congressional oversight and sunsets – all offer a window into the government's use of its powers, and all provide essential protection against abuse.

I welcome all our witnesses and look forward to making progress on these important issues.

444

Testimony of

Andrew C. McCarthy
Senior Fellow
Foundation for the Defense of Democracies
1146 19th St NW - Suite 300
Washington, DC 20036

Before the

United States Senate Judiciary Committee

“Continued Oversight of the USA PATRIOT Act”

Tuesday, May 10, 2005 at 9:30 a.m.
Senate Dirksen Building, Room 226

EFF Section 215-1055

Chairman Specter, Senator Leahy, and members of the Judiciary Committee, thank you for inviting me here this morning. It is an honor to testify before this Committee, particularly on a matter of such importance to our national security.

I am currently an attorney in private practice in the New York area and a Senior Fellow at the Foundation for the Defense of Democracies, a non-partisan, non-profit policy institute here in Washington that is dedicated to defeating terrorism and promoting freedom. For close to eighteen years up until October of 2003, I served as an Assistant United States Attorney in the Southern District of New York.

While I held several executive staff positions in our Office and had the opportunity to participate in a number of significant cases, the most important work that I participated in, along with teams of dedicated Assistant United States Attorneys working arm-in-arm with our colleagues in the FBI and other federal and state law enforcement agencies, was in the area of counterterrorism.

From a time shortly after the World Trade Center was bombed on February 26, 1993, through early 1996, I was privileged to lead the prosecution against Sheik Omar Abdel Rahman and eleven others for conducting against the United States a war of urban terrorism that included, among other things: the WTC bombing, the 1990 murder of Meir Kahane (the founder of the Jewish Defense League), plots to murder prominent political and judicial officials, and a conspiracy to carry out what was called a "Day of Terror" – simultaneous bombings of New York City landmarks, including the United Nations complex, the Lincoln and Holland Tunnels (through which thousands of commuters traverse daily between lower Manhattan and New Jersey), and the Jacob K. Javits Federal

Building that houses the headquarters of the FBI's New York Field Office (a plot that was thwarted).

After defending those convictions on appeal, I also participated to a lesser extent in some of our Office's other prominent counterterrorism efforts – including pretrial litigation in the prosecution against the bombers of the U.S. embassies in Kenya and Tanzania, and the appellate defense of convictions in the case involving the conspiracy to bomb Los Angeles International Airport during the Millennium observance. Finally, following the 9/11 attacks, I supervised the U.S. Attorney's command post in lower Manhattan, near ground zero, working closely with all our colleagues in the law enforcement and intelligence communities to try to do what we have been trying to do ever since that awful day: prevent another attack against our homeland.

I have not been in the trenches for a few years, but it is from the trenches that I come. And it is from that perspective that I thank this Committee, and the entire Congress, for its tradition of strong, bipartisan support for protecting our national security.

It was that tradition that caused members of both Houses and both parties to enact the Patriot Act in October 2001 by overwhelming margins. It was a good-potential idea then. Nearly four years later, with no attacks on our homeland since 9/11, we can confidently say it is a good proven idea today. It has been a crucial ingredient in the American people's inoculation against the perilous disease that is militant Islamic terrorism. And it remains good, relatively pain-free protection that we badly need. Just as we do not eliminate or water down vaccines when we are fortunate enough to go three or four years without a major outbreak of disease, it would be foolish, and dangerous, to

eliminate or water down eminently reasonable measures that promote the welfare of the American people.

Much, of course, has been said, pro and con, in our national three-year debate over the Patriot Act. I will later address some of the provisions that are slated to sunset absent new legislation. For present purposes, though, I believe it is more important to confront the larger, thematic issues implicated by our debate. I respectfully submit that a number of the premises on which we are proceeding – and which catalyze ill-conceived efforts, such as the proposed SAFE Act, to dilute the Patriot protections – are simply wrong and cry out for re-examination.

National Security v. Domestic Policing

A constant refrain on the proponent side of any discussion about the Patriot Act has been that, at least insofar as investigative techniques are concerned, what Patriot basically did was bring some old techniques up to date with 21st century technology while – and this is the important point – vesting federal agents conducting national security investigations with powers analogous to what agents conducting criminal investigations have had at their disposal for decades. The Justice Department has made this argument repeatedly. I have made it myself, as have a number of like-minded people, and even those who take the counterpoint on some Patriot provisions have often acknowledged that it is essentially true.

I am not here today to say it is not true – far from it. In retrospect, however, this unassailable point has led us to glide past, almost without notice, a rudimentary question: to wit, *should* national security investigations be akin to criminal investigations? Should they proceed along similar lines with similar assumptions under similar guidelines? The

answer is that they most certainly should not. And simply because the investigative techniques used in both spheres resemble each other does not mean they should be functionally the same in both contexts. The contexts are crucially different.

As former U.S. Attorney General William P. Barr explained in October 2003 testimony before the House Select Committee on Intelligence, in the role of enforcing U.S. law, the executive acts in a field where government has a monopoly on the use of force and seeks to discipline an errant member of the body politic who has allegedly violated its rules. That member, who may be a citizen or an immigrant with lawful status, is vested with rights under the U.S. Constitution. In this ambit, executive action is properly subjected to great constraints: courts are imposed as a bulwark against suspect executive action and in favor of individual liberty; presumptions in favor of privacy and innocence raise the executive's burden, hindering it from taking investigative or prosecutorial action absent convincing evidence of wrongdoing; and defendants, as well as many investigative subjects who have not been charged, enjoy the assistance of counsel, whose task is to make maximal use of the individual's array of rights and privileges -- rendering the government's enforcement and information-seeking efforts more burdensome.

The line our society has drawn here is very clear. We believe it is preferable for the government to fail than for an innocent person to be wrongly convicted or otherwise deprived of his rights. That is our criminal justice system. It is the envy of the world, and we would not want to change it a wit in its basic assumptions for those who are properly in it.

Not so the ambit of national security. In this wider realm, where government confronts a host of sovereign states and sub-national entities (particularly terrorist organizations) who claim the right to use force, the executive is not enforcing American law against a suspected criminal. Rather, government here is exercising national defense powers to protect against external threats and, as Attorney General Barr put it, "preserve the very foundation of all our civil liberties." The galvanizing national concern in this realm is to defeat the enemy and preserve our constitutional order. The line drawn here is that government cannot be permitted to fail – not in the confrontation with forcible threats from without, and not in the confrontation with hostile foreign agents operating within the United States.

The fact that terrorists and terror networks can sometimes be countered by the criminal justice system does not mean that terrorism is a criminal justice problem to be addressed with a criminal justice mindset. We want constitutional rights to protect Americans from oppressive executive action. We do not, however, want constitutional rights to be converted by enemies of the United States into weapons in their war against us. We want courts to be a vigorous check against overbearing governmental tactics in the investigation and prosecution of Americans for ordinary violations of law; but we do not – or, at least, we should not – want courts to degrade the effectiveness of executive action targeted at enemies of the United States who seek to kill Americans and undermine their liberties. And while we would prefer to see guilty drug dealers or racketeers or frauds go free than see a single innocent person convicted of one of those crimes, who among us would really prefer to have terrorists to operate freely, threatening us broadly,

simply to avoid infringements that are generally minor and either exceedingly rare or predominantly hypothetical?

This backdrop is critical to any assessment of the Patriot Act. The tools that Congress gave national security investigators would be considered well within constitutional norms even if we were judging them under the rigorous standards of the criminal justice system. That is the point made by the refrain that Patriot merely put intelligence agents on a par with their colleagues in criminal enforcement. In point of fact, however, we are not talking about domestic policing here. This is national security, and Congress could have done more – and would no doubt do precisely that if the exigencies of an imminent or a completed terrorist assault required it for the protection of the American people.

Thus, for all the rhetoric, the Patriot Act was a measured response to a dire and continuing threat. Watering it down in an effort to bring it more into line with domestic policing, or to deal with hypothetical threats to civil liberties – particularly in the absence, after nearly four years, of any meaningful record of actual violations – would make no sense and would short sell our greater obligation to the collective safety of the American people.

The lack of an empirical record of infringements is telling here. Naturally, it says a great deal about the kind of people we have in the trenches these days – something I will address in a few moments. But it also tells us other important things. First, the Patriot Act is reasonable. If it were unreasonable you'd know it because you could simply point to the way it operated.

Second is the role of oversight and politics – and here, I mean *politics* in the best sense of the word in a well-functioning democracy. The Justice Department does not overreach very often, but when it does in the criminal justice arena, that can't be kept a secret for very long. Even if Justice were not as ethical as it has traditionally been in investigating and disclosing its own missteps, defense lawyers are too skillful and the judiciary too vigilant to permit misfeasance or malfeasance to escape notice and condemnation.

But national security is primarily the responsibility of the political branches. While all criminal justice roads lead to the courthouse, the vast majority of what is done in furtherance of national security is in no way intended for judicial proceedings. Relations between the United States and foreign enemies are a political issue. Discovery procedures under the modern interpretation of due process make trials an impractical response to many, if not most, international enemies – educating them and empowering them to imperil us. Moreover, as the 9/11 Commission, among other investigations, has detailed, the state of our human intelligence is such that we rely heavily on information from foreign intelligence services – vital pipelines that would quickly dry up if those who confided in us came to believe their methods, sources and secrets would be revealed in American court proceedings.

Consequently, even if we were all in agreement that the courts were equipped and suitable to be a major check on the executive's national security powers – and I don't think we will ever have consensus on that – they will never be the primary check. The primary check will always be this Congress. This Congress and the American people.

The best national security is broad discretion in the executive branch to act swiftly and comprehensively against threats to the public welfare. The best defense of civil liberties in the national security arena is not further extending the reach of the judiciary. It is aggressive oversight by Congress, and particularly by this Committee whose members are so well versed in the foreign counter-intelligence operations of the Justice Department and the FBI.

It is this Committee, not the federal courts, which is best equipped to determine whether the Justice Department has, for example, reasonably exercised its authority to compel production of library or hospital records; whether it has misused its license to seek roving wiretaps with less particularity in exigent circumstances; whether it has abused its national security wiretapping authority as a pretext to conduct what in reality is a criminal investigation.

Some contend that relying too much on congressional oversight and not enough on courts will return us to the bad old days of abuses of power, of spying on those who pose no threat and are merely exercising their First Amendment right to dissent, and other dark chapters of the past. I respectfully submit, however, that this gives too little credit to our collective capacity to learn from our errors and our scandals. It is because of that past that executive branch officials are well-aware of what they may not do, and of what they should avoid – when possible – even the appearance of doing. It is because of that past that Congress is well aware of what must be watched and what questions must be asked. And it is because of that past that we all know what the American people, who so cherish their civil liberties, will not tolerate.

I respectfully submit that reaching the ideal for which we are all striving, an America that is both truly safe and truly free, is dependent on remaining mindful of these critical differences between domestic policing and national security. Those who challenge some of the Patriot Act provisions – especially those scheduled to sunset – have raised important issues and legitimate concerns about the vibrancy of our liberties. In virtually every case, however, the prudent course is to renew the Patriot powers with a commitment to searching oversight that relies on the expertise of Congress and the good sense of the American people as our best protection. It is not to remove or restrict necessary powers – powers that are being exercised responsibly – on the off chance that they might at some point be abused.

The Targets and Effects of Regulation

Because there is such scant evidence of Patriot Act authorities actually being abused, much of the debate about the Act has been hypothetical. So it is posited: What if agents, to satisfy nothing but their presumed prurient interests, were to snoop into the reading, viewing and Internet habits of Americans? What if agents, freed from requirements to be specific about either the person or location of a roving wiretap application, were to eavesdrop on all conversations in a large building, or a city block, or a whole town? What if agents, unable to generate enough evidence to justify a regular criminal wiretap, were to pretend their subjects were national security threats as a pretext to using FISA wiretap authority? And so on.

These are the types of what-ifs on which our regulating proceeds: The presumption that absent this or that prohibition or hurdle, the default position of agents will be disregard, if not outright contempt, for individual rights. Even further blinking

reality, it is presumed that these over-extended officials (in the FBI's case, some percentage of about 11,000 agents seeking to protect nearly 300 *million* Americans) in fact enjoy a leisurely existence, and thus that absent laws precluding or restricting various investigative activities, they have not merely the inclination but also the time to pry into the personal and constitutionally protected activities and interests of ordinary Americans.

Perhaps – although I doubt it – there is a place for such skepticism in the arena of domestic policing, where, as I mentioned earlier, such a premium is placed on avoiding conviction and other infringements against the innocent. But there is simply no place for it in the realm of protecting the welfare of the American public from hostile forces. More to the point, the presumption is delusional.

The agents and Justice Department attorneys who are the objects of our concern here are far from perfect. They are human beings thrust into a challenging, high-stakes, stressful calling in which tough judgment calls have to be made, often on the fly and never in the perfect calm of hindsight. Errors are inevitable – and I say that as one who has made more than his share. But as a rule, they are the polar opposites of rogues. They are honorable and conscientious. They got into this line of work out of a sense of duty and a desire to protect people's rights, not transgress them. They are Americans themselves who care deeply about civil liberties. They are, due to their work, more knowledgeable about and cognizant of the Constitution than most Americans – the Constitution they take an oath to uphold; an oath that, in my experience, they tend to take very seriously.

With due respect to all involved, I believe the Patriot Act debate has overlooked this root reality. As a result, the American people are being presented a distorted view of

what goes on in the FBI field offices and U.S. Attorney's offices throughout the country where the rubber meets the road.

As a rule, agents and government attorneys tend to be cautious – sometimes too cautious, as we have learned through such inquiries as the 9/11 Commission and the February 2003 Interim Oversight Report to this Committee by Senators Leahy, Grassley and Specter. It is not an unusual thing for a prosecutor to be awaked in the wee hours by a call from agents in the field who want to verify before taking needed action that they will not be stepping over the line by making an arrest or conducting a search. Most day-to-day investigative decisions require consultation and at least one supervisory rung of approval; more unusual tactics require approvals up several rungs of the chain-of-command – and some even call for inter-agency approval; and virtually anything that legally calls for an application to the Foreign Intelligence Surveillance Court (FISC) will be scrubbed by lawyers at the FBI and the Justice Department before it ever gets there.

Agents and attorneys are overworked. Investigations of international terror networks and other enemies of the United States are large and complex. They often call for mastery of voluminous intelligence materials and open source materials, as well as familiarity with the vagaries of legal systems across the globe. They are challenged by the immense difficulty of getting accurate information about facts on the ground in remote parts of the world, and even in our own country given the quantity and very uneven quality of foreign language translations.

And there is tremendous stress. A mistake in a drug investigation may mean a shipment gets through. Similarly, some omission in a fraud investigation may cause an innocent victim lots of money, while an investigative error in a violent gang case may

cost a victim his life. All of these problems – the risks criminal investigators live with on a daily basis – are bad, but they are manageable. National security is different in degree as well as kind. The terrorists who confront us have already killed thousands of Americans, have cost our society untold billions of dollars, and have impelled us to place brave young American men and women in harm's way overseas. We know that the terrorists are not done. We know that they not only threaten us still but that they seek weapons of a destructive capacity that could literally dwarf the impact of the 9/11 atrocities. The price of a mistake in this thicket is incalculable, and the pressure to avoid such a mistake is an enormous one that our dedicated agents and government attorneys bear every day.

This is our reality. The government officials whose conduct, actual and potential, is at the heart of our inquiry here are not anything near Big Brother. They are not even slightly interested, as a general matter, in what Americans are reading or what websites they are accessing. They are not desirous of poring over personal healthcare or financial information unrelated to some good-faith investigative imperative. In point of fact, in this information age, they are awash in data and severely challenged to sort the wheat from the chaff – which is to say: they don't have enough time to read and process the things we actually want them to read and process.

It would be counterfactual and perilous to legislate based on the assumption that honorable people will behave badly. It is also unbecoming. When a federal court is confronted with a claim that Congress has acted unconstitutionally in passing a piece of legislation, it operates with a presumption of regularity – it deferentially assumes that Senators and Representatives who enact bills and Presidents who sign them do so

mindful and respectful of their constitutional obligations. When sovereign states regard each others' official acts and judgments, they similarly and appropriately do so with a presumption of regularity. This hardly means mistakes are never made or that these presumptions are never overcome. But it is a salient aspect of the dignity that impels our society to respect its institutions – the very respect which undergirds the rule of law – that we operate from a premise that our officials are neither reckless nor roguish, and that they act responsibly.

I respectfully submit that the agents and government attorneys who are sworn to uphold the law should be entitled to nothing less. The stakes here are high, implicating not only the safety of Americans but also their civil liberties. Consequently, it is imperative that Congress perform its crucial oversight function to ensure that the broad powers wielded by the executive branch are wielded appropriately. But our law should presume regularity. It should not erect a priori bars or unwarranted hurdles to the government's access to information that may save lives based on a badly flawed assumption that the power of access will be systematically abused.

Again, I am not saying mistakes will not be made. Investigation is a human process, meaning missteps are inevitable. We have very fine people on the front lines, so fortunately the mistakes are relatively infrequent. But they do inevitably happen. Sometimes, such as in the case of Mr. Mayfield in Portland, the mistakes will be egregious and embarrassing. Nevertheless, no set of laws, however carefully tailored to promote civil liberties, is going to repeal error. Meanwhile, in the national security context, it is simply a fact that every legislative measure fashioned to meet real or imagined violations of individual liberty necessarily renders less certain the public's

equally significant – indeed, more significant – communal right to safety. Making a power more difficult to use inevitably results in its being used less often, and in at least some failures to use it when it is needed. We have already seen this unavoidable rule of human nature play out prior to the 9/11 attacks, particularly in the context of the regulatory wall that obstructed information flow between intelligence agents and criminal investigators (which I will address later). We will not connect the dots if we make it needlessly difficult to know what the dots are.

Finally, if Congress legislates counterfactually, assuming government officials will be rogues unless they are hemmed in by laws more exacting than the Constitution demands, it is worth a commonsense appraisal of what that accomplishes. Rogues are not merely rare; they are rogues exactly because they will flout the rules regardless of what the rules are. Bad faith actors cannot be effectively regulated; they need to be weeded out and dispensed with. To the contrary, the only officials who are actually impacted when laws are passed making their tasks more difficult are the vast majority of honorable ones – the ones who will conscientiously try to follow the rules no matter what the rules are. These, of course, are the ones whom it was unnecessary to target with more burdensome rules in the first place because their default position is a healthy respect for the constitutional rights of their fellow Americans.

Rules, moreover, have a dynamism in practice that – and I say this with the utmost respect – sometimes seems lost on those who enact them. Responsible officials will not, as a rule, operate on the margins of their authority. They will be fearful of even the appearance of stepping over the line. It is a fact of bureaucratic life that whatever officials may technically be authorized to do, they will in practice do less of, so to avoid

suspicion or criticism. Indeed, it has been observed with some force by raconteurs of life under the aforementioned "wall," including the Foreign Intelligence Surveillance Court of Review, that perhaps more damaging than the regulations themselves was the ethos instilled by the regulations – the seeping conceit that certain investigative activity had been made more difficult precisely because it was inherently unseemly and thus to be avoided whenever possible.

If, for example, you make it more difficult to get a business record, a pen register, or a roving wiretap, you will in practice find that some number – perhaps a large number – of business records, pen registers and roving taps that you believed your legislation authorized, and that you as the public's representatives would want agents to seek, will not be sought. As a practical matter, no one's individual liberties will have been advanced in any meaningful way, but the public's collective safety may be gravely imperiled because information that might have disrupted terrorism will have been missed.

The record demonstrates that the powers vested in agents and government attorneys by the Patriot Act were necessary and have been used judiciously. This should come as no surprise; indeed, we should have expected nothing less. Concerns about abuse are hypothetical, but they are not unimportant and should be handled, as they have been handled for nearly four years, by vigilant congressional oversight. Laws that have helped protect the American people from a repeat of 9/11 should not be diluted.

I will proceed to address some of the Patriot Act provisions that are currently scheduled to sunset at the end of this year. As time is short, I will not endeavor to address all of them but will be prepared to discuss them if the Committee believes that will be helpful.

Business Records: Section 215¹

None of the Patriot Act's enhancements of government's investigative arsenal has been more assiduously libeled than Section 215. Indeed, in the public mind, it has become the "library records" provision notwithstanding that libraries are nowhere mentioned. While there are points of legitimate concern, most of the controversy is a tempest in a teapot. Section 215 is a good law. It merits being made permanent, albeit with some tailoring to provide expressly for the now-implicit ability of production-order recipients to seek judicial narrowing. Beyond that, altering this provision out of overwrought suspicions about potential abuse would likely, and perversely, result only in greater potential abuse.

Section 215 modified FISA in two ways. The first relates to what information may be compelled. Formerly, this was restricted to travel, lodging and storage records. Section 215 broadens the scope to include not merely such business records but "any tangible things (including books, records, papers, documents, and other items)."

This is not nearly as dramatic as it appears. For decades, Rule 17(c), Fed.R.Crim.P, has authorized compulsory production of "any books, papers, documents, data, or other objects" to criminal investigators *by mere subpoena*. Given the incontestable breadth of the federal criminal statutes implicated by terrorism and espionage, coupled with the broad license grand juries have to conduct investigations, there is no item now obtainable by Section 215 that could not already be compelled by

¹ This discussion of Section 215, and subsequent discussions of Sections 214 and 218, are adapted from essays I contributed to a series of written debates on the Patriot Act sponsored by the American Bar Association (in particular, its Standing Committee on Law and National Security). The debates are available at <http://www.patriotdebates.com>, and are scheduled to be released in book form, copyrighted by the ABA, later this month.

simple subpoena (and thus made accessible to intelligence agents, who are now permitted to share grand jury information).

Why such extensive access with virtually no court supervision? Because the items at issue here are primarily activity records voluntarily left in the hands of third parties. As the Supreme Court has long held, such items simply do not involve legitimate expectations of privacy. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 744 (1979). This renders them categorically different from the private information at issue in the context of search warrants or eavesdropping, in which the court is properly imposed as a bulwark, requiring a demonstration of cause before government may pierce established constitutional safeguards that are the entitlement of American citizens and many aliens.

Thus while the Patriot Act plainly expanded FISA powers, the reality is that prior law governing national security investigations was unnecessarily stingy, especially in contrast to rules that empower criminal agents probing far less serious matters, like gambling. Such incongruities are intolerable in the post-9/11 world, where public safety is critically dependent on intelligence.

Here, one must address the theater over library records, risibly evoking visions of DOJ Thought Police monitoring, and thus chilling, the reading preferences of Americans.² First, as demonstrated above, government has long had the authority to compel reading records by subpoena; yet there is no empirical indication of systematic prying into private choices – else we'd surely have heard from the robustly organized librarians. Second, leaving aside that agents (who are also Americans) generally lack

² *See, e.g.,* ACLU release, July 22, 2003: "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." (Quoted at DOJ Patriot Act website, "Dispelling the Myths," http://www.lifeandliberty.gov/subs/add_myths.htm#s215).

voyeuristic interest in the public's reading and viewing habits, investigations in the Information Age are simply too demanding for such shenanigans. Naturally, one could never eliminate the occasional rogue – no matter what precautions were in place; but in the 21st Century, voluminous information streams and finite resources leave no time for this sort of malfeasance. Third, and most significantly, it does not diminish our society's high regard for personal liberty to observe that an *a priori* ban on investigative access to reading records would be both unprecedented and dangerous.

In point of fact, 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). Possession of jihadist writings is also relevant in the cases of accused terrorists who, having pled not guilty, put the government to its burden of proving knowledge and intent.

More importantly, as Deroy Murdock of the Hoover Institution (and my colleague at *National Review Online*) has recently detailed in two important articles,³ at least seven of the nineteen 9/11 hijackers in fact made liberal use of libraries in the United States and Europe in the run-up to the attacks. Others, including Junaid Babar who pled guilty last year to providing material support to terrorists, and the infamous Unabomber, Theodore Kaczynski, are known to have used libraries to carry out their crimes. We simply cannot afford to allow libraries to be a terrorist safe harbor in our midst.

³ See "On Borrowed Time – Terrorists use libraries. Law enforcement should be vigilant in the stacks" (NRO May 3, 2005) (<http://www.nationalreview.com/murdock/murdock200505030804.asp>); "Check This Out – Libraries should be a key target of the Patriot Act" (NRO April 25, 2005) (<http://www.nationalreview.com/murdock/murdock200504250750.asp>).

Of course we don't want FBI agents snooping around libraries for no good reason; but do we really want terrorists immunized from the properly prejudicial effects of probative evidence – the type of evidence that has proven key to past convictions? Americans value many species of privacy but sensibly allow them to be overcome when relevant evidence of even minor crime is at stake. It would be extremely unwise to create hurdles for library evidence that don't exist for items stored in a person's own bedroom, or to create impediments in national security cases that don't exist in, say, routine drug investigations.

The second major change wrought by Section 215 involves the showing required before a FISA production order is issued. Previously, agents were called on to provide "specific and articulable facts giving reason to believe that" the records pertained to an agent of a foreign power. Now, the order must issue upon the government's representation that it seeks to obtain intelligence concerning non-U.S. persons, or to protect against international terrorism or espionage.

Practically speaking, this change is, again, less dramatic than appears on the surface. Consider the contrast: in criminal investigations, there is no court supervision at all over government's issuance of subpoenas. Section 215, moreover, expressly prohibits FISA investigations based "solely on ... activities protected by the First Amendment"; criminal probes carry no such protection.

Concededly, however, defenders of Section 215, rather than explaining why court supervision of investigations would be improper, tend counterproductively to stress the court-order requirement. Illustrative is the Justice Department's highlighting that "Section 215 requires FBI agents to get a *court order*." (See "Dispelling the Myths";

www.lifeandliberty.gov/subs/add_myths.htm#_Toc65482101 (emphasis in original). Though accurate, this assertion may inadvertently imply searching judicial review. In fact, Section 215 provides no such thing: if the government makes the prescribed representations, the FISA court is without discretion to deny the order. This is precisely as it should be, but people who have assumed a degree of judicial scrutiny understandably become alarmed upon learning it is a false assumption.

Yes, Section 215's judicial exercise is ministerial, but that does not make it unique or inconsequential. It is analogous to familiar pen register law, under which a judge must issue the authorization upon the request of criminal investigators, with no demonstration of cause. Why? Because our system is premised on separation of powers. Investigation is an executive function. The judicial role is not to supervise the executive but to protect U.S. persons against improper invasions of *legitimate expectations of privacy*. People do not have such expectations regarding the phone numbers they dial, thus a ministerial judicial role is appropriate: the order issues on the court's power, but it is not the judiciary's place to question bona fides of a co-equal branch carrying out its own constitutional function.

In matters of national security more than any other investigative realm, it is crucial to remain mindful of the court's institutional competence. The judiciary's limited role is to protect established constitutional interests, not create new ones as a means to micromanage investigations. When neither U.S. persons nor legitimate expectations of privacy are involved, as is generally the case with Section 215, a court has no cause to demand an explanation of the basis for the FBI's application.

So why require going to the court at all? Because, as is the case with grand jury subpoenas (which are court orders though issued without court supervision), it is appropriate that the directive to comply comes from the judicial power. Moreover, Section 215 prudently charges Congress with the responsibility of ensuring that the executive branch is not abusing its authority. By requiring the FBI to make solemn representations to the court, and mandating that the Attorney General report semi-annually on this provision's implementation, Section 215 provides suitable metrics for oversight and, if necessary, reform.

Finally, the formerly mandated articulation hinders proper investigations. Emblematic is the pre-9/11 Zacharias Moussaoui scenario. There are times when the FBI will have solid reason to suspect that a person is a terrorist operative (as Moussaoui's flight school behavior aroused suspicion), but not yet have developed enough evidence to tie the suspect to a particular foreign power (such as al Qaeda). In such a case, given that the Fourth Amendment poses no obstacle to the FBI's access to third party records, the safety of Americans assuredly should not be imperiled for the benefit of a non-U.S. person by burdening investigators with a legally unnecessary showing it may be difficult, if not impossible, for them to meet.

Section 215 should be amended to clarify that order recipients may move the FISA court to quash or narrow production. This remedy is available in the analogous context of grand jury subpoenas, the Justice Department has appropriately taken the position that it is implicit in Section 215, and it will incentivize investigators to minimize their applications responsibly.

Further modification would be legally unnecessary, as well as unwise policy. Raising the access bar would simply encourage government to proceed by grand jury subpoena or national security letter -- guaranteeing less judicial participation, more difficult congressional oversight, and the inefficiency of quash litigation in district courts throughout the country, rather than in the FISA court (a salient reason for whose creation was to develop specialized expertise in the sensitive issues unique to intelligence investigations).

Arguments that we should grant carve-outs from government access for certain types of records in deference to individual interests in financial and health-care privacy, or the privacy of reading and Internet viewing habits already addressed above, are unwise because they give short shrift to the national security threat. If we were not actually facing a public safety challenge, such individual privacy interests might sensibly be elevated. We need, however, to be at least equally concerned with the collective rights of Americans. National security is the highest *public* interest and the most profound duty of government. When it is truly threatened, as it is now, it makes no sense to give individual interests primacy over the public's need to have foreign enemies thoroughly investigated -- particularly when the Supreme Court has made plain that there are no expectations of privacy in third-party records.

Another frequent and understandable complaint about Section 215 revolves around its so-called "gag rule," which prohibits recipients to disclose the fact of a subpoena. To be sure, the desirability of openness as a check on government overreaching is unassailable if national security is not threatened. A public safety threat, however, requires reasonable balance between the public interest in disclosure and the

reality that disclosure makes our enemies, to be blunt, more efficient at killing us. It can alert them to the fact of an investigation which may thwart our ability to identify key players and locations that threaten Americans. It may endanger the lives of informants or dry up other crucial sources of information (such as wiretaps) since, once terrorists – or, for that matter, members of any criminal organization – realize the government knows enough to seek certain records, their first priority often becomes attempting to determine how they have been compromised.⁴ Finally, it may trigger a planned attack. On this last score, it is again important to note that terrorists are not like other criminals. They are not in it for the money, and they are not as apt to flee and live to fight another day if they believe their cover is blown. Many of them are devoted to their missions to the point of committing suicide to accomplish them. Publicly revealing an investigation before agents have reached the point of being able to thwart an ongoing terrorist plot may serve to accelerate the terrorist plot.

The appropriate balance here, as argued above, is to presume that Justice Department personnel will perform their functions honorably, but to expect searching congressional oversight to ensure that the government is not misusing Section 215. It bears observing that, as a practical matter, the vast majority of third-party subpoena recipients have no interest in disclosure. Given the stakes involved, any modification of the gag rule should put the onus on the few who do to explain why they should not remain mum.

⁴ Among the most damning evidence against Sheik Omar Abdel Rahman in the case I tried several years ago was his energetic effort to figure out how his jihad organization had been infiltrated, triggered by the arrest of fugitive World Trade Center bomber Mahmud Abouhalima in Egypt. In its aftermath, phones and apartments were checked for eavesdropping devices and potential informants were identified and rigorously interrogated.

Pen Registers – Section 214

Issues flowing from the Patriot Act pen register provision, Section 214, are closely related to the business records provision, Section 215. Section 214 sensibly extends the pen register/trap-and-trace device procedures already available for telephone communications to the newer technologies of email and Internet. Importantly, this does not permit government to invade the content of communications; all that is at stake here is routing and addressing information.

Prior FISA law required government to certify that the monitored communications would likely be those either of an international terrorist or spy involved in a violation of U.S. criminal law, or of an agent of a foreign power involved in terrorism or espionage. This was an unnecessary and imprudently high hurdle. The Supreme Court, as noted above, has long held that pen registers do not implicate *any* Fourth Amendment interests – they are not searches, they do not invade legitimate expectations of privacy, and there is no constitutional reason to require investigators to seek court authorization for them at all.

Consequently, Section 214's modification of prior law is both modest and eminently reasonable. Agents are still required to obtain a court order before installing a pen register. In addition, they are still required to make a solemn representation to the court. Now, however, that representation is limited to certifying that the information sought would be relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

Though less extensive than before, this still easily passes constitutional muster. It is also comfortably analogous to criminal practice, where investigators must be granted

pen register authority upon merely certifying that “the information likely to be obtained is relevant to an ongoing criminal investigation[.]” (18 U.S.C. Section 3122(b)(2)). And, as was the case with Section 215, Section 214 may not be employed to conduct an investigation based solely on activities protected by the First Amendment – a safeguard that does not exist in criminal investigations.

Section 214 should neither be modified nor permitted to sunset.

The Wall – Section 218

No subordination of national security to hypothetical fears of civil liberties abuse was more emblematic of the pre-9/11 world than the metaphorical “wall” erected to obstruct the information flow between intelligence and criminal investigators.

Section 218 of the Patriot Act dismantled this construct by amending its literal underpinning – the basis for the ill-conceived “primary purpose” test by which FISA was misinterpreted for nearly a quarter-century, to disastrous effect. As the wall was founded on a skewed interpretation of law, Section 218 was theoretically unnecessary. Nevertheless, it was entirely appropriate and its enactment proved to be critical.

Post-9/11, discussions focus on explaining the genesis of the wall rather than defending it. Indeed, former Attorney General Janet Reno, who did not originally erect the wall but on whose watch it was heightened and solidified in internal Department guidelines, testified to the 9/11 Commission that, more critical to national security than realigning the intelligence community would be “to knock down walls, to promote the sharing of information, and to enhance collaboration in the fight against terrorism.” And in

2002, the Foreign Intelligence Surveillance Court of Review, in its first ever opinion, provided a detailed explanation of the wall's fatal flaws.⁵

The relevant history traces to the 1978 enactment of FISA.⁶ A reaction to Vietnam and Watergate era domestic-intelligence abuses, FISA authorizes the specially created FISC to regulate and monitor the executive branch's conduct of electronic surveillance and physical searches in the context of national security investigations. This is in contrast to ordinary investigations, where the use of those techniques is governed by the criminal law.

In the latter, agents must present probable cause of a crime to obtain a warrant. FISA, on the other hand, is not principally about rooting out crime; it is about national defense, targeting foreign enemies, including international terrorists. Thus, rather than requiring probable cause of a crime, FISA permitted government to "obtain foreign intelligence information" if "there is probable cause to believe that ... the target of the electronic surveillance is a foreign power or an agent of a foreign power[.]"

The difficulty here is that any theoretical divide between *criminal* and *intelligence* matters would not track reality. Espionage, for example, is both a dire national security issue and a felony. Similarly, terrorists commit many crimes (*e.g.*, immigration fraud, identity theft, money laundering, seditious conspiracy, possession of precursor explosives, and bombing, to name just a few) in the course of plotting and attacking. Thus, whether an agent's investigative authority comes from FISA or the criminal law, what emerges is evidence that constitutes *both* national security intelligence and proof of quotidian crimes.

⁵ See <http://www.fas.org/irp/agency/doi/fisa/fiscr111802.html>.

⁶ Title 50, United States Code, Sections 1801et seq. ((2000 ed.)).

This should pose no problem. Agents conducting a proper investigation uncover information. Free to compare notes and study multiple options for dealing with threats to public safety, they can wisely choose the approach that makes the most sense in light of the entire informational mosaic. Prosecution of a crime will get a dangerous person off the street and, equally important, may motivate him to cooperate about the inner workings of a terror network. On the other hand, sustained monitoring might reveal the nature of a terror enterprise while allowing government to prevent attacks without triggering disclosure obligations that attend a prosecution (which educate terrorists about the state and sources of government's intelligence). Plainly, national security dictates a fully informed strategy, taking advantage of the tactics that best fit the circumstances. Prior to 9/11, however, development of such a strategy was hamstrung by a hypothetical and wrong-headed concern: *viz.*, that permitting use in criminal cases of FISA-generated evidence might induce agents to resort to FISA when their "real" purpose was to conduct a criminal investigation.

This was irrational. First, the existence of a crime or national security threat is an objective reality, entirely independent of the investigators' subjective mindsets about why they are investigating. As for agent motivation, our concerns should be whether they have a good reason for investigating and whether the facts they present to a court are accurate. If those things are so, and agents happen to uncover evidence they did not anticipate finding, that should be cause for celebration, not suppression. Thus, it has for decades been the law that (i) evidence of Crime A is admissible even if it was seized in the execution of warrant based on probable cause to believe Crime B had been

committed; but (ii) evidence of a crime is suppressed if the probable cause predicated its seizure was dependent on intentional misstatements of material fact.

Second, it is not sensible to suspect systematically dishonest resort to FISA. FISA applications require a specialized and rigorous internal approval process before presentation to the court. Assuming for the sake of argument (and against the facts in all but the most aberrant of circumstances) an agent willing to act corruptly, it would be far easier and less detectable for such an agent to fabricate the evidence necessary to get an ordinary criminal wiretap than to fabricate probable cause to believe the subject is a national security threat so that FISA may be employed.

Finally, FISA as written posed no obstacle to the use of FISA evidence for criminal prosecution. From a national security perspective, this made eminent sense given the aforementioned propensity of terrorists to commit crimes and the consequent centrality of prosecution as a means to win cooperation and thus secure vital intelligence.

Regrettably, this common sense came unmoored over time. FISA required that a high executive branch official – typically, the FBI director – represent that “the purpose” of the investigation was to obtain foreign-intelligence information (as opposed to building a prosecution). This was simply intended to be a certification; it did not purport to restrict either the scope of the investigation or the permissible uses of any resulting evidence. Unfortunately, soon after FISA took effect, the Justice Department began construing the certification not as a mere *announcement of purpose* but as something more restrictive: a *substantive limitation* on the use of FISA evidence in criminal cases.

As the Review Court opinion elaborated, over time this erroneous interpretation of the certification requirement led to a “false dichotomy”: a futile endeavor to sort

FISA-derived information into the purportedly distinct categories of mere intelligence and criminal evidence. Moreover, given the government's apparent fear that there might be impropriety in the acquisition of criminal evidence via FISA, it should have come as no surprise that the federal courts, too, began fashioning safeguards not found in FISA's text. Thus was born the "primary purpose" test, under which FISA-derived evidence could not be used in criminal prosecutions unless the government demonstrated that its primary purpose had been to collect intelligence, not build a criminal case.

To the contrary, as the Review Court held in 2002, FISA as enacted "clearly did *not* preclude or limit the government's use ... of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution." (Emphasis in original.) But rather than challenge the primary purpose test, the Justice Department bolstered it, by internal 1995 regulations, into the finished product that is now commonly referred to as "the wall." This procedural edifice instructed "the FBI and Criminal Division [to] ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the [foreign intelligence (FI) or counterintelligence (FCI)] investigation toward law enforcement objectives."

As already discussed, this directive, the Review Court found, was "narrowly interpreted" to "prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing FI or FCI investigations." The guidelines and the ethos they forged effectively cut intelligence investigators off not only from criminal agents but also from Assistant United States Attorneys who, by virtue of investigating

and prosecuting several terrorism cases in the 1990's, were among the government's best resources regarding al Qaeda and its affiliates.

The best known pernicious consequence of all this occurred in August 2001. Relying on the wall, FBI headquarters declined to allow criminal investigators to assist an intelligence investigation seeking to locate probable terrorists Khalid al-Midhar and Nawaf al-Hazmi. A few weeks later, on 9/11, the pair helped hijack Flight 77 and pilot it into the Pentagon.⁷

Section 218 makes a seemingly small but crucial adjustment: it guts the primary purpose test by requiring a government to certify that foreign intelligence is merely a *significant* purpose, rather than *the* purpose, for the FISA application. This strikes the correct balance: It recognizes that there is nothing inherently wrong with collecting criminal evidence by FISA, but ensures that FISA will not be employed unless there is some worthy national security purpose.

Section 218 was perhaps legally unnecessary. The Justice Department, after all, could, absent legislation, have changed its internal guidelines and argued that FISA had been misconstrued. Yet, it was certainly appropriate and wise for Congress itself to address a key cog of pre-9/11 intelligence failure. Furthermore, given that the FISA court, post-9/11, improperly attempted to institute the wall procedures as an exercise of judicial supervision, it was no doubt immensely significant to the Court of Review – in reversing the FISA court in 2002 – that the wall had been rejected not just by DOJ but by an act of Congress that carried the force of law.

⁷ See Stewart Baker, "Wall Nuts" (Slate Dec. 31, 2003) (<http://slate.msn.com/id/2093344/>).

Section 218 is vital. The sunset should be removed, and the provision should otherwise remain as is.

Roving Wiretaps – Section 206

Roving wiretaps – that is, multi-point electronic surveillance targeted at persons rather than particular communications devices (e.g., telephones or computers) – have been available to criminal investigators for nearly twenty years. As one would expect, there seems to be consensus that they should be available in national security cases as well, and that was accomplished by Section 206 of the Patriot Act. It has been contended, however, that the roving tap authority is too broad, particularly after additional changes to FISA wrought by the 2002 Intelligence Authorization Act, and that the authority should be narrowed. I respectfully submit that these concerns are overwrought and that Section 206 should remain as is.

The central complaint about FISA roving wiretaps is two-fold. First, it is alleged that they do not require stringent identification of the person who is the target of the surveillance – that is, FISA permits a target whose identity is not known to be described rather than identified.⁸ Second, roving taps are sometimes claimed to be insufficiently particular to satisfy Fourth Amendment muster because they are issued without “particularly describing the place to be searched.” Although that contention would seem to be fatally undermined by the fact that federal appellate courts have upheld roving wiretaps over particularity challenges in the criminal context, critics seize on the fact that

⁸ FISA Section 105(e)(1)(A).

FISA does not contain a safeguard found in the criminal wiretap statute: the so-called "ascertainment requirement."⁹

Both these claims are underwhelming, especially viewed in practical terms. It bears remembering that a FISA roving tap cannot be approved by the FISC unless the government satisfies a judge that there is probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power. Moreover, the warrant may not issue unless the FISC is also convinced there is probable cause to believe that the facilities to be surveilled are being used, or are about to be used, *by that target*. Thus, even absent apodictic identification of the target, it is inconceivable that a description could be so vague and imprecise as to be rendered meaningless, as critics allege, and yet still meet the high, dual-pronged probable cause standard. The Justice Department is not apt to allege, and a federal judge is even less apt to find, probable of terrorist agency and likely use of communications facilities with respect to a target who cannot be described with a reasonable degree of confidence.

The "ascertainment" argument is not persuasive. This requirement in the criminal electronic surveillance law calls for agents, in certain circumstances, not to begin monitoring until they are reasonably certain that the target is in the place where eavesdropping is to occur. But even in the criminal context it is applied only to "oral" communications — i.e., those captured by an eavesdropping device (a "bug") hidden in a location — not to "wire" and "electronic" communications over telephone lines or the

⁹ Title 18, United States Code, Section 2518(12).

Internet.¹⁰

By suggesting that the ascertainment requirement be extended to wire and electronic communications in FISA, critics are thus seeking *greater* constraints on agents conducting national security investigations than on agents doing investigations of ordinary crimes (even comparative trifles like gambling). This makes little sense given the grievous stakes involved and the fact that, if push came to shove, it is dubious, to say the least, that the Constitution (as opposed to FISA) would require any warrant at all for the executive branch to eavesdrop on a foreign enemy operative plotting sabotage against the United States – especially if the operative was a non-U.S. person who lacked a sufficient basis to claim Fourth Amendment protection.¹¹

Section 206's searching judicial review, bolstered by the afore-described probable cause requirements, strikes the right balance between civil liberties and national security. It also imposes a minimization regime which provides that surveillance must stop upon the monitor's determination that innocent conversation has been intercepted – further protecting innocent Americans from undue invasions of privacy. These elements,

¹⁰ See Title 18, United States Code, Section 2518(12), which limits the ascertainment requirement therein to communications falling under Section 11(a), which, in turn, applies only with respect to "an oral communication"; cf. Section 11(b), which applies to "a wire or electronic communication," and note that the Section 12 ascertainment requirement does not deal with Section 11(b).

¹¹ Warrants must be sufficiently particular where they are required. But the Fourth Amendment does not proscribe *warrantless* searches; it proscribes *unreasonable* searches. There would be nothing unreasonable about a search conducted without any warrant – let alone an exquisitely particular warrant – if it targeted a foreign enemy operative bent on doing grave harm to the United States. Indeed, such judicial warrants were not called for until FISA was enacted in 1978. Presumptively, FISA is permitted by the Constitution (I don't believe it has ever been challenged on separation of powers grounds), but it is plainly not mandated by the Constitution. In any event, the Fourth Amendment's particularity requirement should be unavailing for a non-U.S. person – especially one who is a hostile operative of a foreign enemy or terrorist organization. See *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) (holding that the Fourth Amendment did not protect non-Americans from a search by U.S. agents of property outside the United States, and observing that "aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country") (emphasis added); *Kwong Hai Chew v. Colding*, 344 U.S. 590, 597 (1953) ("[t]he alien, to whom the United States has been traditionally hospitable, has been accorded a generous and ascending scale of rights as he increases his identity with our society") (emphasis added).

combined with responsible oversight by Congress, clearly work: there is no record of abuse of roving wiretap authority in the national security context in the nearly four years it has been available.

Given the adequacy of these checks, the urgent need to develop intelligence on terrorists operating domestically, and the peril in which lost information could place Americans, Section 206 is appropriate as written. It should be renewed.

Conclusion

The Patriot Act has been a crucial component of our nation's post-9/11 success in countering the terrorist threat. The investigative powers it granted were measured and respectful of civil liberties. They have been exercised responsibly, as we should have expected they would be and as we should expect they will continue to be. They have been vigilantly and appropriately monitored by this Committee, other congressional committees, and the courts.

On the domestic front, the best antidote to terrorism is robust executive authority checked by searching congressional oversight. I respectfully submit that this is what we have now. It would be a mistake to dilute the Patriot Act powers in response to hypothetical concerns about civil liberties abuse. Given the threat we face and the carnage we have endured, it would be a mistake we cannot afford.

I thank the Committee for its time and attention.



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 3, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

During the closed session of the Senate Judiciary Committee on April 12, 2005, you requested additional information regarding Section 213 of the USA PATRIOT Act. Specifically, you inquired about examples of where the "seriously jeopardizing an investigation" prong was the sole "adverse result" used to request delayed notice. In addition to Operation Candy Box, which was detailed in our April 4, 2005, letter to the Committee, we have described seven additional cases below. It is important to note that the twenty-eight instances cited in our April 4 letter do not equate to twenty-eight investigations or cases. For example, some of the cases that used delayed-notice search warrants utilizing the "seriously jeopardize" prong involved multiple search warrants.

As we are sure you will agree, the following examples of the use of delayed-notice search warrants illustrate not only the appropriateness of the Department's use of this important tool, but also its criticality to law enforcement investigations.

Example #1: Western District of Pennsylvania

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 revealed and endangered a related Title III wiretap that was ongoing for major drug trafficking activities. Originally, the Department was granted a ten-day delay by the court, but the Department sought and was granted eight extensions before notice could be made.

An Organized Crime Drug Enforcement Task Force ("OCDETF"), which included agents from the Drug Enforcement Administration (DEA), the Internal Revenue Service, and the Pittsburgh Police Department, as well as from other state and local law enforcement agencies, was engaged in a multi-year investigation that culminated in the indictment of

the largest drug trafficking organization ever prosecuted in the Western District of Pennsylvania. The organization was headed by Oliver Beasley and Donald "The Chief" Lyles. A total of fifty-one defendants were indicted on drug, money laundering and firearms charges. Beasley and Lyles were charged with operating a Continuing Criminal Enterprise as the leaders of the organization. Both pleaded guilty and received very lengthy sentences of imprisonment.

The Beasley/Lyles organization was responsible for bringing thousands of kilograms of cocaine and heroin into Western Pennsylvania. Cooperation was obtained from selected defendants and their cooperation was used to obtain indictments against individuals in New York who supplied the heroin and cocaine. Thousands of dollars in real estate, automobiles, jewelry and cash have been forfeited.

The case had a discernable and positive impact upon the North Side of Pittsburgh, where the organization was based. The DEA reported that the availability of heroin and cocaine in this region decreased as the result of the successful elimination of this major drug trafficking organization. In addition, heroin overdose deaths in Allegheny County declined from 138 in 2001 to 46 in 2003.

While the drug investigation was ongoing, it became clear that several leaders of the drug 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 Fed Ex package that contained fraudulent credit cards. Had the search into the credit card fraud investigation revealed the ongoing drug investigation prematurely, the drug investigation could have been seriously jeopardized. The credit card investigation ultimately resulted in several cases including US v. Larry Goolsby, Sandra Young (Cr. No. 02-74); US v. Lasaur Beeman, Derinda Daniels, Anna Holland, Darryl Livsey and Kevin Livsey (Cr. No. 03-43); US v. Gayle Charles (Cr. No. 03-77); US v. Scott Zimmerman, Lloyd Foster (Cr. No. 03-44). All of the defendants charged with credit card fraud were convicted except one, Lloyd Foster, who was acquitted at trial. These cases have now concluded.

Example #2: Western District of Texas

The Justice Department executed three delayed notice searches as part of an OCDBTF investigation of a major drug trafficking ring that operated in the Western and Northern Districts of Texas. The investigation lasted a little over a year and employed a wide variety of electronic surveillance techniques such as tracking devices and wiretaps of cell phones used by the leadership. The original delay approved by the court in this case was for 60 days. The Department sought two extensions, one for 60 day and one for 90 days both of which were approved.

During the wiretaps, three delayed-notice search warrants were executed at the organization's stash houses. The search warrants were based primarily on evidence

developed as a result of the wiretaps. Pursuant to section 213 of the USA PATRIOT Act, the court allowed the investigating agency to delay the notifications of these search warrants. Without the ability to delay notification, the Department would have faced two choices: (1) seize the drugs and be required to notify the criminals of the existence of the wiretaps and thereby end our ability to build a significant case on the leadership or (2) not seize the drugs and allow the organization to continue to sell them in the community as we continued with the investigation. Because of the availability of delayed-notice search warrants, the Department was not forced to make this choice. Agents seized the drugs, continued our investigation, and listened to incriminating conversations as the dealers tried to figure out what had happened to their drugs.

On March 16, 2005, a grand jury returned an indictment charging twenty-one individuals with conspiracy to manufacture, distribute, and possess with intent to distribute more than 50 grams of cocaine base. Nineteen of the defendants, including all of the leadership, are in custody. All of the search warrants have been unsealed, and it is anticipated that the trial will be set sometime within the next few months.

Example #3: District of Connecticut

The Justice Department used section 213 of the USA PATRIOT Act in three instances to avoid jeopardizing the integrity of a pending federal investigation into a Connecticut drug trafficking organization's distribution of cocaine base and cocaine. The provision was used to place a global positioning device on three vehicles.

These applications were submitted in the case of *United States v. Julius Moorning, et al.* That case was indicted at the end of April 2004, and 48 of 49 individuals charged have been arrested. As of this date, 38 of the defendants have entered guilty pleas, and several more are being scheduled. The trial of the remaining defendants is scheduled to begin on June 15. All defendants with standing to challenge any of the orders obtained have entered guilty pleas.

The Justice Department believed that if the targets of the investigation were notified of our use of the GPS devices and our monitoring of them, the purpose of the use of this investigative tool would be defeated, and the investigation would be totally compromised. As it was, the principals in the targeted drug-trafficking organization were highly surveillance-conscious, and reacted noticeably to perceived surveillance efforts by law enforcement. Had they received palpable confirmation of the existence of an ongoing federal criminal investigation, the Justice Department believed they would have ceased their activities, or altered their methods to an extent that would have required us to begin the investigation anew.

In each instance, the period of delay requested and granted was 90 days, and no renewals of the delay orders were sought. And, as required by law, the interested parties were

made aware of the intrusions resulting from the execution of the warrants within the 90 day period authorized by the court.

Example #4: Western District of Washington

During an investigation of a drug trafficking organization, which was distributing cocaine and an unusually pure methamphetamine known as "ice," a 30-day delayed-notice search warrant was sought in April 2004. As a result of information obtained through a wiretap as well as a drug-sniffing dog, investigators believed that the leader of the drug distribution organization was storing drugs and currency in a storage locker in Everett, Washington. The warrant was executed, and while no drugs or cash was found, an assault rifle and ammunition were discovered. Delayed notice of the search warrant's execution was necessary in order to protect the integrity of other investigative techniques being used in the case, such as a wiretap. The investigation ultimately led to the indictment of twenty-seven individuals in the methamphetamine conspiracy. Twenty-three individuals, including the leader, have pled guilty, three are fugitives, and one is awaiting trial.

Example #5: Southern District of Illinois

The Justice Department used section 213 of the USA PATRIOT Act in an investigation into a marijuana distribution conspiracy in the Southern District of Illinois. In particular, in November 2003, a vehicle was seized pursuant to authority granted under the provision.

During this investigation, a Title III wiretap was obtained for the telephone of one of the leaders of the organization. As a result of intercepted telephone calls and surveillance conducted by DEA, it was learned that a load of marijuana was being brought into Illinois from Texas. Agents were able to identify the vehicle used to transport the marijuana. DEA then located the vehicle at a motel in the Southern District of Illinois and developed sufficient probable cause to apply for a warrant to search the vehicle. It was believed, however, that immediate notification of the search warrant would disclose the existence of the investigation, resulting in, among other things, phones being "dumped" and targets ceasing their activities, thereby jeopardizing potential success of the wiretaps and compromising the overall investigation (as well as related investigations in other districts). At the same time, it was important, for the safety of the community, to keep the marijuana from being distributed.

The court approved the Department's application for a warrant to seize the vehicle and to delay notification of the execution of the search warrant for a period of seven days, unless extended by the Court. With this authority, the agents seized the vehicle in question (making it appear that the vehicle had been stolen) and then searched it following the seizure. Approximately 96 kilograms of marijuana were recovered in the search. Thirty-

one seven-day extensions to delay notice were subsequently sought and granted due to the ongoing investigation.

As a result of this investigation, ten defendants were ultimately charged in the Southern District of Illinois. Seven of these defendants have pled guilty, and the remaining three defendants are scheduled for jury trial beginning on June 7, 2005.

Example #6: Eastern District of Wisconsin

In a Wisconsin drug trafficking case, a delayed-notice search warrant was issued under section 213 because immediate notification would have seriously jeopardized the investigation. In this case, the Department was in the final stages of a two-year investigation, pre-takedown of several individuals involved in the trafficking of cocaine. The Department initially received a delayed-notice search warrant for seven days, and thereafter received three separate seven-day extensions. For each request, the Department showed a particularized need that providing notice that federal investigators had entered the home being searched would compromise the informant and the investigation.

On February 14, 2004, the United States Attorney's Office for the Eastern District of Wisconsin requested a search warrant to look for evidence of assets, especially bank accounts, at a suspect's residence as well as to attach an electronic tracking device on a vehicle investigators expected to find in the garage. The purpose of the device would be to track the suspect and observe his meetings in the final weeks before the takedown. The warrant also requested delayed notice, based on the particularized showing that providing notice that federal investigators had entered the home would compromise an informant and the investigation. The court issued the search warrant and granted the delayed notification for a period of seven days. On February 15, 2004, authorized officers of the United States executed the search warrant on the subject premises. However, agents were unable to locate the vehicle to install the electronic tracking device.

Before the expiration of the initial delayed-notice period, the Department sought an extension of the delay based on the showing that notice would compromise the informant and the investigation. The court granted a seven-day extension, but investigators were still unable to locate the suspect's vehicle during this time. During this period, however, five suspects were charged with conspiring to possess more than five kilograms of cocaine, and arrest warrants were issued for each of the individuals.

After the issuance of the arrest warrants, the Department sought its third delay of notice to allow agents to endeavor to install the electronic tracking device and to attempt to locate the five suspects. Once again, the request was based on the showing that notice would compromise the informant and the investigation. The court granted another seven-day extension, and agents were able to find a location where one suspect appeared to be staying. After locating the suspect, and before the expiration of the delayed-notice

period, the government requested a separate warrant for this location and for other locations used by the conspirators. The Department also requested its fourth and final delay in the notice period to allow agents to execute the search warrants sought, and to arrest the suspects. The court granted all requests and the suspects were subsequently arrested. As required by law, notice of the searches was given upon arrest.

Example #7: Eastern District of Washington

In a drug trafficking and money laundering case in the State of Washington, a delayed-notice search warrant was issued under section 213 because immediate notification would have seriously jeopardized the investigation. In this case, a district judge had authorized the interception of wire and electronic communications occurring over four cellular telephones that were being used in furtherance of drug trafficking and/or money laundering activities. On December 18, 2004, more than one month after the Drug Enforcement Administration (DEA) began surveillance, DEA agents administratively seized a black Ford Focus owned by one of the suspects based on the determination that the vehicle likely contained controlled substances.

On December 21, 2004, the DEA requested a warrant to search the seized vehicle for drugs, and the court issued the warrant based on the DEA's articulation of probable cause. On the same day, the search warrant was executed on the suspect's vehicle, which was still in the DEA's possession pursuant to the administrative seizure. During the search, agents located approximately two kilograms of suspected cocaine and three pounds of suspected methamphetamine. At the time, the service copy of the search warrant was "served" on the vehicle.

Due to the nature of the investigation, which included the orders authorizing the interception of wire and electronic communications to and from a number of cellular telephones, the DEA believed that both the continued administrative seizure of the vehicle and notice of the execution of the search warrant would greatly compromise the investigation. Therefore, the DEA requested an order allowing them to remove the served copy of the warrant from the vehicle, and delay notice to the owner for sixty days in order to avoid jeopardizing the ongoing criminal investigation. The court granted the order, concluding that immediate notification would compromise a major drug trafficking and money laundering investigation.

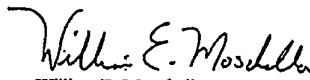
Approximately twenty-five individuals have been indicted as a result of this investigation (eight of whom are still fugitives), and trial is scheduled for this October.

485

In closing, the Department of Justice believes it is critical that law enforcement continue to have this vital tool for those limited circumstances, such as those discussed above, where a court finds good cause to permit the temporary delay of notification of a search.

We hope the information provided above is helpful. Should you require any further information, please do not hesitate to contact this office.

Sincerely,



William B. Moschella
Assistant Attorney General

cc: The Honorable Patrick Leahy
Ranking Minority Member



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 6, 2005

The Honorable Pat Roberts
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

At a hearing before the Senate Select Committee on Intelligence on April 19, 2005, Mr. James X. Dempsey provided testimony to the Committee questioning the Department's use of section 213 of the USA PATRIOT Act relating to delayed-notice search warrants. Specifically, Mr. Dempsey's written statement to the Committee on behalf of the Center for Democracy and Technology says "one of the clearest abuses of the PATRIOT Act is the government's admitted use of Section 213 sneak and peek authority in non-violent cases having nothing to do with terrorism...[including] an investigation of judicial corruption, where agents carried out a sneak and peek search of a judge's chambers..." Because of Mr. Dempsey's allegations, the Committee has asked the Department to provide additional information for the Committee's consideration.

The judicial corruption case Mr. Dempsey refers to was originally identified by the Department in an October 24, 2003, letter to Senator Stevens ("Stevens letter") that detailed the efficacy of delayed-notice search warrants (enclosed). Specifically, the Stevens letter provided the following description of a 1992 public corruption investigation code-named "Court Knot":

In a judicial-corruption case, a court issued a delayed-notice warrant to search the target's judicial chambers and photocopy a "fix book" kept in the desk of the judge's clerk. The book detailed past and future cases which had been fixed or which were to be fixed, and included lists of defendants "to be found guilty." Execution of the warrant resulted in probable cause to set up audio and video surveillance of the chambers. Three court personnel eventually were convicted of civil rights violations.

The matter in question, United States v. Walter Cross, Jules Melograne, and Nunzio Melograne, Criminal No. 94-233, Western District of Pennsylvania, was a federal public integrity investigation involving case-fixing in Allegheny County Common Pleas Court in Pennsylvania, and specifically targeted the chambers of Senior Common Pleas Judge Raymond L. Scheib of the Court of Statutory Appeals, which heard all appeals of summary offenses. Prior to seeking court approval for conducting a search of the judge's chambers, the government had information

establishing probable cause that the judge's clerk and other court personnel kept a fix book of pending cases. It was important to get a copy of the fix book in order to demonstrate to a federal judge that cases were pre-determined. Obviously, records of contacts relating to past cases had little evidentiary value because if confronted, both the corrupt state court officials and any guilty defendants listed would merely (and potentially successfully) assert that the court had properly handled those cases. Because ex post analysis would simply not be sufficient in this unique situation, we needed to be able to demonstrate ex ante that "the fix was in." Prosecutors reasoned a copy of the fix book would allow them to monitor the outcomes of listed cases and, by showing the outcomes were pre-determined, they could clearly demonstrate to a federal judge probable cause to get a wiretap and electronic surveillance.

Upon examination of the fix book, investigators discovered that the conspirators were so bold as to indicate the outcomes of cases by including explicit notations, like "to be found guilty" next to pending defendants names. This served as evidence that cases were pre-arranged to convict defendants in blatant violation of their most basic civil liberties. With the evidence from the fix book, the government was able to establish probable cause for a wiretap and electronic surveillance, even without having a cooperating witness to the conspiracy.

It was evidence obtained as a result of the wiretap and electronic surveillance that was essential to being able to successfully prosecute these corrupt judicial officers. Had we been required to provide immediate notice to the target of the search and seizure of the fix book, it would have precluded our ability to obtain a viable wiretap and electronic surveillance. In other words, it would have tipped off the court personnel that we were onto their scheme. The likely result would have at least been a chance for them to change their activities and further facilitate their contempt for the rule of law. Instead, delayed notice allowed us to demonstrate corruption and was instrumental in obtaining solid evidence to convict these corrupt officials.

This matter resulted in the convictions of three individuals of civil rights violations. All three were initially sentenced to 33 months imprisonment. Following appeal, the sentences of Walter Cross, the head clerk, and Jules Melograne, a senior Magistrate, were reduced to 27 months' imprisonment. Nunzio Melograne, a docket clerk who played a lesser role and had serious health problems, passed away before re-sentencing. More importantly though, we were able to remove corrupt public officials, thus instilling public confidence in our justice system and ensuring innocent people are not convicted of crimes they did not commit. Few things are as important to the mission of the Justice Department as rooting out public corruption. Like terrorism, this is an instance where we can all be thankful the investigators had the ability to delay notification of a search -- a valuable technique that enables the ends of justice.

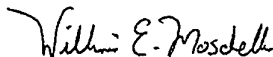
It is worth noting that the search Mr. Dempsey is referring to actually occurred in 1992, almost a decade before the USA PATRIOT Act was passed. Thus, he is inaccurate both in his portrayal of this investigation as an "abuse" and as a USA PATRIOT Act case. In this case, the original warrant and request for authorization for delayed notice were presented to a United States District Court Judge, rather than to a magistrate judge. The government based its request for

delayed notice upon prior decisions in other Circuit Courts. See United States v. Villegas, 899 F.2d 1324, 1336-1337 (2d Cir.), cert. denied, 498 U.S. 991 (1990); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986); United States v. Johns, 851 F.2d 1131 (9th Cir. 1988); and United States v. Pangburn, 983 F.2d 449 (2nd Cir. 1993).

Additionally, the government filed regular reports with the District Court, detailing the ongoing investigation and need for continuing non-disclosure. The entire non-disclosure issue was subject to continuous court review, and was successfully litigated before another District Court Judge, as a pretrial suppression issue. As the Department has often said, and as the Stevens letter indicated, 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. Section 213 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.

We have enclosed some of the relevant court documents for additional information. If you have additional questions about this or any other issue related to the USA PATRIOT Act, please don't hesitate to contact this office.

Sincerely,



William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable John D. Rockefeller IV
Vice Chairman

STATEMENT BY SENATOR KEN SALAZAR IN SUPPORT OF THE SECURITY
AND FREEDOM ENHANCEMENT (SAFE) ACT OF 2005

For insertion into the record of the Senate Judiciary Committee for May 10, 2005

Mr. Chairman, I appreciate the opportunity to submit the following statement into the Committee's record for today's hearing on the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. I also want to thank Ranking Member Leahy and the other members of the Judiciary Committee for their willingness to accommodate me this morning. And I especially want to thank Senator Craig and Senator Durbin for their leadership on the important issues before the Committee today, and for their graciousness in allowing me to be part of their efforts.

Although I am not a member of the Senate Judiciary Committee, I served as Attorney General for the State of Colorado for six years, and have first-hand experience with regard to many of the issues that fall under your jurisdiction. In fact, the experience I gained during my tenure as Colorado's Attorney General is one of the reasons I have the privilege of being an original cosponsor of legislation directly related to the topics being discussed at today's hearing: the Security and Freedom Enhancement (SAFE) Act of 2005.

Let me be clear: I firmly believe we need to provide our nation's law enforcement agencies with the tools they need to effectively investigate and prosecute would-be terrorists, and the provisions of the USA PATRIOT Act have gone a long way toward accomplishing that goal. As Attorney General, I worked with law enforcement officials from all over my state – representing areas ranging from metropolitan Denver to the rural San Luis Valley – to give them the resources and authority they needed to serve at the front lines in the war against terrorism. I know first-hand how important many of the new authorities the PATRIOT Act provided were in enabling these individuals to effectively perform their duties.

Having said that, I also recognize that preserving the basic civil liberties we enjoy as Americans is central to upholding the fundamental rule of law in this country. In ensuring that law enforcement has what it needs to protect freedom, we need to be extremely careful not to infringe on that freedom ourselves by creating a situation where the government can potentially invade the privacy of innocent citizens. Toward that end, the SAFE Act would take a number of important steps toward clarifying and strengthening those sections of the PATRIOT Act that pose the greatest threat to innocent Americans' fundamental rights and freedoms.

Specifically, our legislation would establish a more thorough review process with respect to the sections of the PATRIOT Act that authorize delayed notification of search warrants, record searches under the Foreign Intelligence Surveillance Act (FISA), and the use of National Security Letters. Our bill would also seek to prevent instances where law enforcement can conduct surveillance on innocent Americans by placing reasonable

limitations on the use of roving wiretaps and trap and trace devices, and require increased public reporting about how law enforcement has used many of the powers granted under the PATRIOT Act.

I am confident that, by working in good faith and across party lines, Congress can reauthorize the PATRIOT Act in a way that provides law enforcement with the resources and investigative authority it needs without unnecessarily compromising Americans' rights and freedoms. As an original cosponsor of the SAFE Act, I am proud to be a part of the effort to strike this balance in the Senate. I am deeply grateful to Senators Craig and Durbin for allowing me that privilege, and look forward to working with others on the Committee in whatever capacity I can to help move the process forward.

Again, I thank Chairman Specter, Ranking Member Leahy, and the other distinguished members of the Committee for the opportunity to submit my remarks.

United States Senate
WASHINGTON, DC 20510

SENATE BILL OF RIGHTS CAUCUS
STATEMENT OF PRINCIPLES

Whereas, the American people want Congress to strike a careful balance, protecting civil liberties while giving the government the powers it needs to fight the war on terrorism;

Whereas, when the government seeks expanded powers, the burden of proof is on the government to demonstrate that such powers are necessary to combat terrorism;

Whereas, it is the constitutional duty of members of the Senate to review thoroughly legislative proposals that expand government powers, such as the USA PATRIOT Act, to ensure that they materially enhance security, that they include adequate checks and balances, and that they will not lead to violations of civil liberties;

Now, therefore, the *Senate Bill of Rights Caucus* is hereby established to:

- 1) Serve as a forum for Senators to examine legislative proposals that expand government powers, such as the USA PATRIOT Act, to ensure that they materially enhance security, that they include adequate checks and balances, and that they will not lead to violations of civil liberties; and
- 2) Educate Senators about such legislative proposals and about the importance of protecting civil liberties as we fight the war on terrorism.

GRASSROOTS OPPOSITION TO THE USA PATRIOT ACT
381 Communities and States (58 million people) as of May 5, 2005

*Alaska	San Francisco	*Idaho	Lexington	Lewis & Clark	New York	Texas
Anchorage	San Jose	Boise	Lincoln	City	N Hempstead	Austin
Bathel	San Mateo Cty	Idaho Cty	Littleton	Missoula	Nyack	Dallas
Denali Borough	San Rafael	Moscow	Lowell	Whitefish	Plattsburgh	El Paso
Fairbanks	San Ramon	Illinois	Manchester-by-	Nebraska	Rosendale	Sunset Valley
Fairbanks N. Star	Santa Barbara	Carbondale	the-Sea	Lincoln	St. Lawrence Cty	Utah
Borough	Santa Clara	Chicago	Marblehead	Lincoln	Schenectady	Castle Valley
Gustavus	Santa Clara Cty	Evanston	Milton	Nevada	Schuyler Cty	*Vermont
Homer	Santa Cruz	Glencoe	Newton	Eiko	Syracuse	Athens
Juneau	Santa Cruz Cty	Oak Park	North Adams	Eiko Cty	Tompkins Cty	Braintreeboro
Kansai	Santa Monica	Indiana	Northampton	New Hampshire	Urbana	Burlington
North Pole	Saratoga	Bloomington	Oak Bluffs	Exeter	Westchester Cty	Dummerston
Sika	Sausalito	Bloomington	Orleans	Farmington	Woodstock	Guilford
Skagway	Sebastopol	Iowa	Peabody	Marlborough	North Carolina	Jamalca
Soldotna	Soledad	Ames	Pittsfield	Peterborough	Boone	Marlboro
Valdez	S. Pasadena	Des Moines	Provincetown	Portsmouth	Camboro	Montpelier
Arizona	S. Pasadena	Kansas	Rockport	New Jersey	Chapel Hill	Newfane
Bisbee	Tehama Cty	Kansas City/	Shutesbury	Englewood	Davidson	Putney
Flagstaff	Ukiah	Wyandotte Cty	Somerville	Ewing	Durham	Rockingham
Jerome	Union Cty	Lawrence	Sudbury	Franklin Twp	Durham Cty	Waitsfield
Pima Cty	Watsonville	Kentucky	Swampscott	Highland Park	Greensboro	Warren
Tucson	W. Hollywood	Lexington-	Tisbury	Keansburg	Orange Cty	Westminster
California	Yolo Cty	Lexington-	Truro	Borough	Raleigh	Windham
Alameda Cty	Colorado	Fayette Cty	Wollfleet	Lawrence Twp	Ohio	Virginia
Albany	Aspen	*Maine	Wendell	Mercer Cty	Cleveland	Alexandria
Ahambra	Boulder	Bangor	West Tisbury	Montclair Twp	Heights	Arlington Cty
Arcata	Carbondale	Mount Vernon	Westford	Mullica	Obertin	Charlottesville
Barkley	Crestone	Orono	Weston	Passaic Cty	Oxford	Falls Church
Calistoga	Dacono	Portland	Michigan	Pelerson	Toledo	Richmond
Clatsmont	Denver	Waterville	Ann Arbor	Phillipsburg	Yellow Springs	Washington
Contra Costa Cty	Durango	Maryland	Auburn Hills	Plainfield	Oregon	Bainbridge Island
Cotati	Fort Collins	Baltimore	Detroit	Princeton	Ashland	Bellingham
Davis	Oak Creek	Greenbelt	East Lansing	Borough	Astoria	Clallam Cty
Duarte	Paonia	Montgomery Cty	Fondale	West Windsor	Benton Cty	Corvallis
Dublin	Ridgway	Prince George's	Grand Rapids	Willingboro	Douglas Cty	King Cty
El Cerrito	San Miguel Cty	City	Ingham Cty	New Mexico	Eugene	Olympia
Emeryville	Telluride	Takoma Park	Kalamazoo	Albuquerque	Oroville	Port Townsend
Fairfax	Ward	Massachusetts	Lake Cty	Aztec	Gaston	Riverside
Glendale	Connecticut	Lathrup Village	Lansing	Bayard	Lane Cty	San Juan Cty
*Hayward	Bethany	Meridian Tsp.	Acton	Farmington	Multnomah Cty	Seattle
Humboldt Cty	Hampden	Pontiac	Amherst	Grant Cty	Port Orford	Snoqualmie
Lake Cty	Hartford	Southfield	Aquinnah	Las Vegas	Talent	Tacoma
Livermore	Mansfield	Troy	Arlington	Los Alamos Cty	Wheeler	Tonaskee
Los Angeles	New Haven	Minnesota	Ashfield	Rio Arriba Cty	Pennsylvania	Turnwater
Los Gatos	Delaware	Duluth	Brewster	Santa Fe	Berks County	Twisp
Marin Cty	Arden	Minneapolis	Brookline	Silver Cty	Eno	Vashon-Maury
Mendocino Cty	Newark	Robbinsdale	Buckland	Socorro	Lansdowne	Island
Mill Valley	Wilmington	St. Paul	Cambridge	Taos	Philadelphia	Whatcom Cty
Monte Sereno	Florida	Mississippi	Carlisle	Valencia Cty	Pittsburgh	Washington,
Mountain View	Alachua Cty	Jackson	Charlemon	New York	Reading	D.C.
Nevada City	Broward Cty	Missouri	Chatham	Albany	Wilkinsburg	West Virginia
Oakland	St. Petersburg	Kansas City	Chilmark	Albany Cty	York	Huntington
Pacific Grove	Sarasota	St. Louis	Colrain	Bathlehem Twp	Rhode Island	Wisconsin
Palo Alto	Tampa	University City	Concord	Canton	Charlestown	Douglas Cty
Pasadena	Georgia	*Montana	Conway	Danby	Middletown	Eau Claire
Pinole	Atlanta	Beaverhead Cty	Dennis	Elmira	New Shoreham	Madison
Placer Cty	Savannah	Bozeman	Duxbury	Greenburgh	N. Providence	Milwaukee
Pleasanton	*Hawaii	Butte-Silver Bow	Eastham	Huntington	Providence	Wyoming
Porterville	Honolulu	Dillon	Edgartown	Ithaca	S. Kingstown	Fremont Cty
Richmond	Health	Eureka	Groton	Mount Vernon	Tennessee	
Sacramento	Lenox	Helena	Heath	Town of New	Falitz	
Salinas	Loverett		Lenox	Val. of New Palz		
San Anselmo			Loverett			

Source: Bill of Rights Defense Committee, www.bordc.org

*indicates statewide resolution

**United States Senate
Committee on the Judiciary**

Tuesday, May 10, 2005

**Testimony
of
Suzanne E. Spaulding**

Introduction

Chairman Specter, Senator Leahy, and members of the committee, thank you for inviting me to participate in today's hearing on the USA PATRIOT Act and the legal framework for combating international terrorism.

Let me begin by emphasizing that I have spent over twenty years working on efforts to combat terrorism, starting in 1984 when I had the privilege to serve as Senior Counsel to then Committee member and now Committee Chairman, Senator Arlen Specter, who, as many of you know, in 1986 introduced and guided to enactment the first law to provide extraterritorial jurisdiction over terrorist attacks against Americans abroad.

Over the succeeding two decades, in my work at the Central Intelligence Agency, at both Senate and House intelligence oversight committees, and as Executive Director of two different commissions on terrorism and weapons of mass destruction, I have seen how the terrorist threat changed from one aptly characterized in the mid-80s by Brian Jenkins remark that "terrorists want a lot of people watching, not a lot of people dead," to one that is now better

described by former DCI Jim Woolsey's observation that "the terrorists of today don't want a seat at the table, they want to destroy the table and everyone sitting at it."

There is no question that today we face a determined set of adversaries bent on destroying American lives and our way of life. The counterterrorism imperative is to deny the terrorists both of these objectives. Evaluating how well the USA PATRIOT Act, as enacted and as implemented, satisfies this counterterrorism imperative is the fundamental task for this committee, for the Congress as a whole, and for the American public.

Distinguishing between domestic intelligence operations and criminal law enforcement investigations

One of my greatest concerns about the USA PATRIOT Act and other changes in the law over the last several years is the migration of intrusive criminal investigative powers into the careful legal framework we had established for domestic intelligence collection, which is largely governed by the Foreign Intelligence Surveillance Act (FISA), and a reverse migration of the kind of secrecy and non-disclosure that characterizes intelligence operations into the criminal context of Title 18. Tearing down the wall that hampered the sharing of information between intelligence and law enforcement was essential and I supported it. Nevertheless, there are significant differences in the way that information is collected by intelligence operations as opposed to criminal law enforcement investigations, differences that require particularly careful oversight of any new powers granted in the intelligence context.

2

Intelligence operations, by necessity, are often *wide-ranging* rather than specifically focused—creating a greater likelihood that they will include information about ordinary, law-abiding citizens; they are conducted in *secret*, which means abuses and mistakes may never be uncovered; and they *lack safeguards* against abuse that are present in the criminal context where inappropriate behavior by the government could jeopardize a prosecution. These differences between intelligence and law enforcement help explain this nation's long-standing discomfort with the idea of a domestic intelligence agency.

Because the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigations should be no broader or more inclusive than is absolutely necessary to meet the national security imperative and should be accompanied by rigorous oversight by Congress and, where appropriate, the courts.

Unfortunately, this essential caution was often ignored in the FISA amendments contained in the PATRIOT Act. The authority actually became *broader* as it moved into the intelligence context and oversight was not accordingly enhanced.

Changes to FISA were often justified on the grounds that this authority is already available in the criminal context and “if it’s good enough for use against drug dealers, we certainly should be able to use it against international terrorists.” But in the FISA amendments in sections 214 and 215 of the

PATRIOT Act, for example, we moved from the criminal requirement that information demanded by the government is "relevant to a criminal investigation" to requiring only that information is "relevant to an investigation to protect against international terrorism." Consider this term. It does not say "an investigation into international terrorism activities"—which would at least mean there was some specific international terrorism activity being investigated. Instead, it says "an investigation *to protect against* international terrorism." Imagine if the FBI was engaged in an investigation to protect against bank robbery. What does that mean? Just how broad is that scope? Who's records could not be demanded under such a broad standard?

Conclusion

We often say that democracy is our strength. A key source of that strength stems from the unique relationship between the government and the governed, one based on transparency and trust. Intelligence collection imperatives challenge those democratic foundations and demand rigorous oversight.

These hearings, and your willingness to carefully consider whether provisions adopted in haste at a time of great fear should be renewed or modified, will contribute significantly to restoring the necessary public confidence that the government is protecting both American lives and America's way of life. Thank you for your work and for this opportunity to be here today.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 56

Page 90 ~ Duplicate

Page 91 ~ Duplicate

Page 92 ~ Duplicate

Page 93 ~ Duplicate

Page 94 ~ Duplicate

Page 95 ~ Duplicate

Page 96 ~ Duplicate

Page 97 ~ Duplicate

Page 98 ~ Duplicate

Page 99 ~ Duplicate

Page 100 ~ Duplicate

Page 101 ~ Duplicate

Page 102 ~ Duplicate

Page 103 ~ Duplicate

Page 104 ~ Duplicate

Page 105 ~ Duplicate

Page 106 ~ Duplicate

Page 107 ~ Duplicate

Page 108 ~ Duplicate

Page 109 ~ Duplicate

Page 110 ~ Duplicate

Page 111 ~ Duplicate

Page 112 ~ Duplicate

Page 113 ~ Duplicate

Page 114 ~ Duplicate

Page 115 ~ Duplicate

Page 116 ~ Duplicate

Page 117 ~ Duplicate

Page 118 ~ Duplicate

Page 119 ~ Duplicate

Page 120 ~ Duplicate

Page 121 ~ Duplicate

Page 122 ~ Duplicate

Page 123 ~ Duplicate

Page 124 ~ Duplicate

Page 125 ~ Duplicate

Page 126 ~ Duplicate

Page 127 ~ Duplicate

Page 128 ~ Duplicate

Page 129 ~ Duplicate

Page 130 ~ Duplicate

Page 131 ~ Duplicate

Page 132 ~ Duplicate

Page 133 ~ Duplicate

Page 134 ~ Duplicate
Page 135 ~ Duplicate
Page 136 ~ Duplicate
Page 137 ~ Duplicate
Page 138 ~ Duplicate
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate