Testimony of

Mr. David S. Kris

Senior Vice President
Time Warner, Inc
March 28, 2006

Testimony of David S. Kris before the
Committee on the Judiciary, United States Senate
March 28, 2006

Mr. Chairman, Senator Leahy, and Members of the Committee: Thank you for the opportunity to testify about certain electronic surveillance conducted by the National Security Agency (NSA). As you know, I worked on national security matters, including the Foreign Intelligence Surveillance Act (FISA), when I was at the Department of Justice (DOJ). However, I was not read into the NSA surveillance program, and I have no classified information concerning it.

My testimony is divided into two main parts. The first discusses statutory and constitutional issues raised by the NSA surveillance program. The second part offers some thoughts on possible legislation, including a draft bill and explanation of its main provisions. Both parts of the testimony suffer from my factual ignorance. It is difficult to analyze a surveillance program, and almost impossible to comment on legislation to regulate such a program, without the facts. Caveat emptor.

Statutory and Constitutional Analysis

My statutory and constitutional analysis of the NSA surveillance program can be summarized as follows: (1) NSA engaged in foreign intelligence "electronic surveillance" as defined by FISA ; (2) FISA's "exclusivity provision" prohibits such surveillance except under the "procedures" in FISA; (3) the September 2001 Authorization to Use Military Force (AUMF), as interpreted by the Supreme Court in Hamdi v. Rumsfeld, does not implicitly repeal the exclusivity provision or otherwise authorize the surveillance; and therefore (4) the NSA's surveillance program raises the question whether the exclusivity provision is an unconstitutional infringement of the President's constitutional power under Article II. The answer to that question (and to the related Fourth Amendment question) depends in large part on facts not yet available. I believe, however, that the constitutional analysis will turn in large part on two operational issues - the importance of the information sought (as compared to the scope of the surveillance), and the need to eschew the use of FISA in obtaining the information. With the relevant facts unavailable, I express no opinion on the constitutional issue.

As of this writing, the government's best legal defense of the NSA program appears in a letter from DOJ to certain Members of Congress dated December 22, 2005, and a whitepaper released by DOJ on January 19, 2006. The letter and whitepaper can be summarized as follows: (1) the President has constitutional authority under Article II to "order warrantless foreign intelligence surveillance within the United States" of the type conducted by NSA; (2) that constitutional authority "is supplemented by statutory authority under the AUMF" as interpreted in Hamdi; (3) the NSA surveillance program accords with the exclusivity provision because FISA "permits an exception" to its own procedures where surveillance is "authorized by another statute, even if the other authorizing statute does not specifically amend" the exclusivity provision; and (4) any doubt on the previous question must be resolved in the government's favor to "avoid any potential conflict between FISA and the President's Article II authority as Commander in Chief." Finally, the government asserts in its whitepaper, (5) if the exclusivity provision does forbid the NSA surveillance, then it was repealed by the AUMF or is unconstitutional. In the discussion that follows, I address each of these arguments. While I do not agree with the government, I appreciate the very high quality of its current legal analysis.

I. Did the NSA Conduct Foreign Intelligence "Electronic Surveillance"?

At the outset, it appears that NSA engaged in "electronic surveillance" as defined by FISA. In a briefing held on December 19, 2005, the Attorney General described NSA's conduct as "electronic surveillance of a particular kind, and this would be intercepts of contents of communications where . . . one party to the communication is outside the United States." He also said that FISA "requires a court order before engaging in this kind of surveillance." It is generally "electronic surveillance" under FISA to acquire "the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." The definition is even broader as applied to the targeting of United States persons - e.g., a citizen or green-card holder.

In its whitepaper, DOJ acknowledges that NSA "intercept[ed] international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations." It "assume[s] . . . that the activities described by the President constitute 'electronic surveillance' as defined by FISA," although it also argues that the definition produces some anomalies in light of changing technology and other factors. In any event, there is no way for outsiders to look behind the government's assumption, and therefore no option other than to proceed as if it were true. Following the government's lead, I assume that NSA engaged in "electronic surveillance" as defined by FISA.

II. Did Congress Intend Such Surveillance to be Conducted Solely Under FISA?

A. Constitutional Preclusion.

Congress intended to foreclose the President's constitutional power to conduct foreign intelligence "electronic surveillance" without statutory authorization. A provision of FISA, enacted in 1978 and now codified at 18 U.S.C. § 2511(2)(f), provides in relevant part that "procedures in . . . the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in [FISA] . . . may be conducted." It also provides that the criminal wiretapping law known as "Title III," and other statutes governing ordinary law-enforcement investigations, are "exclusive" as to the surveillance activity that they regulate.

The language of this "exclusivity provision" as a whole could be more elegant, but when read in light of FISA's legislative history, its meaning is hard to avoid. The House Intelligence Committee's 1978 report on FISA explains:

despite any inherent power of the President to authorize warrantless electronic surveillances in the absence of legislation, by [enacting FISA and Title III] Congress will have legislated with regard to electronic surveillance in the United States, that legislation with its procedures and safeguards prohibit[s] the President, notwithstanding any inherent powers, from violating the terms of that legislation.

Congress recognized that the Supreme Court might disagree, but the 1978 House-Senate Conference Committee report expressed an intent to

apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter.' Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952).'"

Indeed, FISA repealed a provision of Title III disclaiming any intent to limit the "constitutional power of the President" in this area. This disclaimer provision, the Supreme Court held in 1972, "simply left presidential powers where it found them." Citing the Court's holding, FISA's legislative history explains that it "does not simply leave Presidential powers where it finds them. To the contrary, [it] would substitute a clear legislative authorization pursuant to statutory, not constitutional, standards. Thus, it is appropriate to repeal this section [of Title III], which otherwise would suggest that perhaps the statutory standard was not the exclusive authorization for the surveillances included therein." In short, FISA was designed "to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." As far as the President's constitutional power is concerned, there is no avoiding the preclusive intent of the exclusivity provision. As I read the government's whitepaper, it agrees with this point.

B. Statutory Preclusion.

The exclusivity provision also exerts a preclusive effect with respect to other statutes. It identifies the "exclusive means" for conducting electronic surveillance without regard to whether that surveillance is premised on legislation or the President's inherent constitutional power. Indeed, one "purpose" of the exclusivity provision was to "set[] forth the sections of the United States Code which regulate the procedures by which electronic surveillance may be conducted within the United States." Put differently, FISA "constitute[s] the sole and exclusive statutory authority under which electronic surveillance of a foreign power or its agent may be conducted within the United States." Congress has continued to respect that standard. When it enacted the Stored Communications Act in 1986, which authorizes conduct that is "electronic surveillance" under FISA, Congress made a corresponding amendment to the exclusivity provision. The exclusivity provision consistently has been understood as a complete list of the statutes under which "electronic surveillance" may be conducted.

Of course, if Congress enacted a new statute expressly authorizing "electronic surveillance," but failed to amend the exclusivity provision, the new statute nonetheless would be given full force and effect. Facing an "irreconcilable conflict" between the new statute and the exclusivity provision, courts likely would overcome their normal aversion, and find an implied repeal (or amendment) of the latter by the former. An ambiguous new statute, however, would be read not to authorize electronic surveillance in order to avoid a conflict with the exclusivity provision. Thus, the statutory question presented here is whether Congress has enacted legislation clearly authorizing the NSA surveillance program and thereby implicitly repealing the exclusivity provision.

C. The Government's Argument.

The government appears to maintain that the exclusivity provision applies only to the President's constitutional power, not to other statutes. In support of that argument, it advances the "commonsense notion that the Congress that enacted FISA could not bind future Congresses." It goes on to urge that "[i]t is implausible to think that, in attempting to limit the President's authority, Congress also limited its own future authority by barring subsequent Congresses from authorizing the Executive Branch to engage in surveillance in ways not specifically enumerated in FISA or [Title III], or by requiring a subsequent Congress to amend FISA and [the exclusivity provision]." Indeed, the government claims, the exclusivity provision can have no preclusive effect on other statutes because of the "well-established proposition that 'one legislature cannot abridge the powers or a succeeding legislature.'"

In my view, this argument mistakes a question of legislative intent for one of legislative power. Congress could authorize electronic surveillance under a new statute at any time, either by explicitly or implicitly amending or repealing the exclusivity provision; there is no need for what the Supreme Court has called "magical passwords" to overcome its preclusive effect on other statutes. As Justice Scalia recently explained, "[a]mong the powers of a legislature that a prior legislature cannot abridge is, of course, the power to make its will known in whatever fashion it deems appropriate," but this doctrine "may add little or nothing to our already-powerful presumption against implied repeals." All that is required is a sufficiently clear statement.

Moreover, as a matter of common sense, it is easy to see why Congress might have wanted the exclusivity provision to apply to other statutes as well as to the President's constitutional power. By enacting a comprehensive list of laws governing electronic surveillance, and declaring the list "exclusive," Congress foreclosed (or sought to foreclose) the President from relying on an ambiguous new provision to claim implicit legislative approval for surveillance conducted in violation of FISA. There is nothing "implausible" in that, given the then-recent history of abuse cited in the Church Report. The government's current reliance on the AUMF - a law that does not mention surveillance - is, of course, a perfect illustration of what the exclusivity provision may have been designed to prevent.

As a fallback, the government maintains that FISA itself authorizes electronic surveillance under any other statute. In other words, it seems to accept that the "procedures" in FISA are indeed "the exclusive means by which electronic surveillance . . . may be conducted." But it claims that "FISA permits an exception" to its own procedures for surveillance "authorized by another statute," and that this exception applies "even if the other authorizing statute does not specifically amend" the exclusivity provision. The government relies on a provision of FISA prescribing criminal penalties for persons who "engage[] in electronic surveillance under color of law except as authorized by statute." It explains that the "use of the term 'statute' here is significant because it strongly suggests that any subsequent

authorizing statute, not merely one that amends FISA itself, could legitimately authorize surveillance outside FISA's standard procedural requirements."

This transitive argument, which moves from the exclusivity provision to FISA's criminal penalty provision, and from there to any and all other surveillance statutes, deprives the exclusivity provision of any operative effect on other legislation. As such, it fails for the reasons stated above: The exclusivity provision applies to statutes as well as to the President's constitutional power. If the transitive argument were correct, Congress would not have needed to list any other statutes, including Title III, in the exclusivity provision, because all would have been incorporated through FISA. The government's "exception" swallows the rule.

The government's argument also fails on its own terms. Taking FISA as a whole, the penalty provision's reference to surveillance "authorized by statute" is best read to incorporate another statute only if it is listed in the exclusivity provision (or, as discussed above, if it effects an implicit repeal or amendment of that provision). That reading retains the operative effect of the exclusivity provision on other statutes and harmonizes the exclusivity and penalty provisions. It also accords with the legislative history of the penalty provision, which describes it as establishing a criminal offense for surveillance "except as specifically authorized in" Title III and FISA, the two statutes listed in the 1978 version of the exclusivity provision.

A related version of the government's argument would be that the penalty provision is "included" in FISA's procedures rather than an "exception" to them. This argument, at least, finds some support in a footnote in FISA's legislative history. In pertinent part, the footnote declares that "the 'procedures' referred to in [the exclusivity provision] include" the procedure of obtaining judicial approval for pen-trap surveillance under Federal Rule of Criminal Procedure 41. Rule 41 is not listed in the exclusivity provision, but the footnote explains that it is included in FISA's procedures "because of the [affirmative] defense" to prosecution in FISA's penalty provision, which applies to surveillance "conducted pursuant to a search warrant or court order." The NSA surveillance, of course, was not conducted pursuant to court order. But if FISA's "procedures" include Rule 41 because of the penalty provision's affirmative defense, the government could argue that they must also include other statutes because of the elements of the penalty provision itself.

The chief difficulty with this argument is that it conflicts with the plain language of the exclusivity provision. That provision's reference to "procedures . . . by which electronic surveillance . . . may be conducted" denotes provisions affirmatively authorizing surveillance, not those prescribing penalties for unauthorized surveillance. Thus, the relevant "procedures" are FISA's rules governing applications to the Foreign Intelligence Surveillance Court (FISC) - a court that enjoys jurisdiction to grant orders "under the procedures set forth in this chapter" - as well as the statute's rules permitting electronic surveillance in certain circumstances without the FISC's approval. FISA's penalty provision does not contain such "procedures" because it does not prescribe means by which surveillance may be conducted. A footnote in legislative history, even in history as authoritative as the House Intelligence Committee's report, cannot overcome the words of the statute. Perhaps for that reason, the courts have not relied on the footnote or adopted the government's argument, despite several opportunities to do so.

D. Constitutional Avoidance.

The government finally relies on the doctrine of constitutional avoidance, arguing that its interpretation must prevail to "avoid any potential conflict between FISA and the President's Article II authority as Commander in Chief." Avoidance doctrine, however, applies only within a range of otherwise permissible constructions - in Justice Scalia's words, it "is a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." Although the government's interpretation is not frivolous, I do not think it is permissible. The exclusivity provision means what it says, and FISA's procedures simply do not incorporate or create an exception for any and all other surveillance statutes. Indeed, there is a certain irony in the government's reliance on avoidance doctrine where, as here, Congress so clearly intended to confront the constitutional question and limit the President's Article II authority. As a doctrine of legislative intent, rather than judicial humility, constitutional avoidance seems wholly inapplicable to the exclusivity provision.

E. Conclusion.

In sum, Congress declared that FISA's procedures are the exclusive procedures for conducting foreign intelligence electronic surveillance. As against the President's constitutional power to conduct such surveillance without adherence to FISA, Congress asserted its own power in opposition. As against other statutes, Congress meant at the very least to require a clear statement before they could be read to authorize such surveillance as an implied repeal or amendment of the exclusivity provision. That is the framework established by FISA in 1978 and upheld by Congress and the President, at least until now.

III. Does the AUMF Authorize the NSA Surveillance?

A. The AUMF.

The government contends that the NSA surveillance is permitted by the Authorization to use Military Force (AUMF), a joint resolution passed by Congress and signed by the President shortly after the September 11, 2001, attacks. In Hamdi v. Rumsfeld, the Supreme Court concluded that the AUMF authorized the use of military detention. Although the AUMF did not refer specifically to such detention, it did authorize the President to use "all necessary and appropriate force" against "nations, organizations, or persons" associated with the September 11 attacks, and the Supreme Court determined that in some situations, detention "is so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use."

It would not be difficult for the government to advance the same argument with respect to intelligence gathering, which - although not as easily characterized as a "use of force" - has always been part of warfare. Electronic surveillance is obviously of more recent vintage, but even FISA's legislative history acknowledges that it has been conducted by all Presidents since technology permitted; electronic surveillance of telegraph signals was apparently conducted as early as the Civil War. DOJ's whitepaper traces this history in detail, and the NSA has published an informative study on the history of signals intelligence in war that makes similar assertions. It is therefore possible to conclude that, in authorizing the President to commit our troops to battle, Congress also implicitly authorized the collection of signals intelligence to aid them. On the logic of Hamdi, electronic surveillance on the battlefield, or perhaps in Afghanistan generally, is fairly within the ambit of the AUMF, at least when the AUMF is read in a vacuum. Surveillance of international communications between the U.S. and Afghanistan (or of domestic communications within the United States made by persons with some connection to the war, which the government asserts it is not acquiring through the NSA program) would obviously be a more difficult assertion, but not necessarily out of the question.

B. The AUMF and Other Laws.

To conclude that the AUMF authorizes (some form of) electronic surveillance when read in a vacuum, however, is not enough because of the atmosphere and circumstances in which it actually was enacted. In September 2001, when the AUMF was passed, Congress was also considering prototypes of what the following month became the USA Patriot Act. The Patriot Act, of course, substantially amended FISA to aid the government's efforts against terrorism. I have not reviewed the legislative history of the Patriot Act for individual remarks supporting or undermining the government's current position, and in any event courts tend to mistrust such subjective indications of congressional "intent." Nonetheless, given the nearly simultaneous Congressional overhaul of FISA, it is hard to read the AUMF as carving out a wide slice of "electronic surveillance" involving U.S. persons and others located in the United States.

It is even harder if, as I believe, the AUMF would effect such a carve-out only if it implicitly repeals the exclusivity provision. In Hamdi, Congress had enacted a statute in 1971 providing that "[n]o citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress." The Hamdi Court found that the AUMF was an "Act of Congress" and that detention pursuant to it therefore satisfied the 1971 statute. As explained above, however, the exclusivity provision does not simply forbid electronic surveillance except pursuant to an Act of Congress; it provides that, with respect to foreign intelligence surveillance, FISA is the only such Act.

Finally, the government's reading of the AUMF also stumbles on another of FISA's provisions. As enacted in 1978, FISA allows a limited exception from its normal rules requiring FISC approval of most surveillance for 15 days immediately following a declaration of war by Congress. In light of that provision, FISA seems a fortiori not to contemplate a permanent or indefinite exception (to some or all of its rules) based on an authorization to use military

force. The idea behind the 15-day period was to give Congress time "for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency." The AUMF certainly was not an explicit amendment to FISA, and as noted above it falls short of effecting an implicit amendment or repeal, particularly because the USA Patriot Act is an explicit amendment to FISA enacted in response to the September 11 attacks.

C. Conclusion.

In sum, I do not believe the statutory law will bear the government's weight. It is very hard to read the AUMF as authorizing "electronic surveillance" in light of the nearly simultaneous enactment of the Patriot Act. It is essentially impossible to read it as repealing FISA's exclusivity provision. And the AUMF suffers further in light of FISA's express wartime provisions. Even with the benefit of constitutional avoidance doctrine, I do not think that Congress can be said to have authorized the NSA surveillance.

IV. Is the NSA Surveillance Unconstitutional?

If FISA and the AUMF do not authorize the NSA surveillance, then a constitutional issue arises. Does the President's Article II power allow him to authorize the NSA surveillance despite the exclusivity provision? That is a very hard question to answer. As Justice Jackson observed in 1952, and as the Court echoed in 1981, there is a "poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves." In this concrete case, where we do not know what NSA was and is doing, legal poverty joins with factual ignorance. The combination hinders efforts to address either the separation-of-powers or the Fourth Amendment issues that are raised here. In the spirit of blind man's bluff, however, I can offer a few tentative observations.

A. Separation of Powers.

It may be useful to begin with the premise that the President has authority, under Article II of the Constitution, to conduct foreign intelligence electronic surveillance, including surveillance of U.S. citizens inside the United States, without a warrant, even during peacetime, at least where he has probable cause that the target of surveillance is an agent of a foreign power. Before FISA's enactment, in the face of Congressional silence, every court of appeals to decide that issue had upheld the President's authority. Similarly, before FISA was amended to authorize foreign intelligence physical searches, it was relatively easy to conclude that the President had inherent authority to conduct such searches. The DOJ whitepaper contains an extensive discussion of these points that I am more or less prepared to accept for present purposes.

The constitutional question presented here, however, is whether the President retains such authority in the face of Congressional efforts to restrict it. It is settled general law, after the Steel Seizure case and Dames & Moore, that "Presidential powers are not fixed but fluctuate, depending upon their disjunction or conjunction with those of Congress." The government accepts this. Thus, the question is not whether the President has inherent authority to conduct electronic surveillance, but whether FISA is unconstitutional in restricting that authority. Is there some hard core of Presidential power that is plenary - i.e., immune from Congressional regulation? And is the NSA surveillance program within that core?

In certain circumstances, at least, there does appear to be a core of plenary Presidential power. Justice Jackson spent the bulk of his famous concurring opinion considering whether President Truman's steel seizure was constitutional despite congressional opposition (he and five other Justices concluded that it was not). The Supreme Court has used two tests to identify plenary powers, neither of which is very illuminating. As a formal matter, the question is whether "one branch of the Government [has intruded] upon the central prerogatives of another." As a functional matter, the question is whether one branch has unduly "impair[ed] another in the performance of its constitutional duties." DOJ appears to agree that these are the relevant tests.

These principles apply to the President's Commander-in-Chief power. For example, the Supreme Court has held that the President may convene courts martial even in the absence of any authorizing statute. Yet Congress also clearly enjoys authority to prescribe standards and procedures for courts martial, based on its Constitutional grant of authority "To make Rules for the Government and Regulation of the land and naval Forces." The Court has said that under this clause Congress "exercises a power of precedence over . . . Executive authority." But could Congress

forbid the President from ever convening a court martial? That seems unlikely given that the "President's duties as Commander in Chief . . . require him to take responsible and continuing action to superintend the military, including courts-martial." Congress could, however, prescribe the factors controlling whether the death penalty may be imposed by a court martial, and the President probably would not be free to disregard those factors.

Other examples can be imagined. Could Congress declare war but order the military not to use airplanes or tanks to prosecute the war? As someone once asked, could Congress in 2003 have enacted legislation directing the Marines to execute a flanking maneuver in the battle for Tikrit? It is hard to see how Congress could do those things, because the use of particular weapons or maneuvers are essentially tactical decisions, at the core of what a Commander in Chief of armed forces must determine. On the other hand, it is probably common ground that Congress could stop appropriations for airplanes or for tanks altogether under its authority to "raise and support Armies" and to "provide and maintain a Navy." Congress sometimes enacts appropriations riders, setting conditions on the President's use of monies, but it is not clear whether Congress can use such riders to accomplish indirectly what it cannot accomplish directly. There are relatively few straight, bright lines in this area.

A real example arises in connection with the treatment of military detainees. After months of publicly-reported negotiations between Vice President Cheney and Senator McCain, Congress in December 2005 passed, and the President signed, a law that would ban the torture of such detainees. However, the President's signing statement explained that he intends to construe the law "in a manner consistent with the constitutional authority of the President to supervise the unitary executive branch and as Commander in Chief and consistent with the constitutional limitations on the judicial power." In other words, while the ban may be tolerable in some (or even most) instances, there may be other instances in which it unconstitutionally restricts the President's power to use torture or other coercive interrogation techniques. In such instances, the President apparently believes, his power to torture is plenary.

All of these real and hypothetical examples illustrate what Professor Corwin famously called the Constitution's "invitation to struggle" for dominance in foreign affairs. Depending on the vigor of the struggling parties, I believe that the constitutional (and perhaps political) validity of the NSA program will depend in large part on two operational questions. The first question concerns the need to obtain the information sought (and the importance of the information as compared to the invasion of privacy involved in obtaining it). To take a variant on the standard example as an illustration of this point, if the government had probable cause that a terrorist possessed a nuclear bomb somewhere in Georgetown, and was awaiting telephone instructions on how to arm it for detonation, and if FISA were interpreted not to allow surveillance of every telephone in Georgetown in those circumstances, the President's assertion of Article II power to do so would be quite persuasive and attractive to most judges and probably most citizens. The Constitution is not a suicide pact.

The second question concerns the reasons for eschewing the use of FISA in obtaining the information. For example, if FISA did not contain an emergency exception, and if a particular surveillance target satisfied the substantive requirements of the statute and absolutely had to be monitored beginning at once, the President's assertion of Article II power to do so for 72 hours while an application was being prepared for judicial approval also would be fairly persuasive. More generally, in this case, I would like to know whether NSA is satisfying all of FISA's substantive standards (e.g., probable cause that the target of surveillance is an agent of a foreign power), even if it is not satisfying all of the statute's procedural requirements (e.g., approval by the FISC or the Attorney General). As discussed in the second part of my testimony, this question bears directly on any proposed legislation.

If NSA is breaching FISA's substantive and procedural standards, and if the surveillance acquires a large amount of private information not directly relevant to its objective, it would likely be met with hostility. A reprise of something like Operation Shamrock, for example, supported by arguments that FISA simply requires too much paperwork, would be very problematic. A lot turns on the facts.

B. Fourth Amendment.

The NSA surveillance program also presents a Fourth Amendment issue. It may be possible to construct an argument that, if the surveillance applies only to international communications intercepted at the border, no Fourth Amendment problem arises. In United States v. Ramsey, the Supreme Court upheld a search without probable cause

or a warrant of international first-class mail as it entered the country. The Court observed that "[b]order searches . . . from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." The Court rejected the argument that, despite this general principle, "mailed letters are somehow different." It explained:

The border-search exception is grounded in the recognized right of the sovereign to control . . .who and what may enter the country. It is clear that there is nothing in the rational behind the border-search exception which suggests that the mode of entry will be critical. . . [C]ustoms officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Surely no different constitutional standard should apply simply because the envelopes were mailed not carried.

It is possible to imagine the government trying to extend this argument from paper mail to electronic mail or even to telephone calls. But it is by no means a sure thing. In any event, as far as I can tell, the government has not advanced the argument to support the NSA surveillance program.

Border exception aside, it is almost impossible to address the Fourth Amendment issue without more facts. In its whitepaper, DOJ explains that "in order to intercept a communication, there must be 'a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.'" In other locations, the whitepaper refers to a "reasonable belief" or its equivalent. Translated into Fourth Amendment terms, this could be viewed as a reference to "reasonable suspicion," which of course is something less than probable cause. On the other hand, in his January 24 prepared remarks at Georgetown University, the Attorney General stated: "Moreover, the standard applied - 'reasonable basis to believe' - is essentially the same as the traditional Fourth Amendment probable cause standard. As the Supreme Court has stated, 'The substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'" The Supreme Court decision quoted by the Attorney General is Brinegar v. United States, a 1949 case with an extended discussion of "probable cause" as used in the criminal law.

Although it may look like nothing more than a semantic squabble, the legal difference between probable cause and reasonable suspicion could be very important. If the President prevails on the separation-of-powers question, then he would (to that extent) have the power to conduct warrantless foreign intelligence electronic surveillance despite FISA, just as the courts had held he did prior to FISA. All of those courts, however, required probable cause that the surveillance target was an agent of a foreign power; none suggested that surveillance is permissible based on reasonable suspicion. As the government points out, those were peacetime decisions evaluating conventional surveillance techniques and technology, and it may be that something less than traditional probable cause is "reasonable" under the Fourth Amendment in wartime or with the advent of new surveillance approaches.

Ultimately, as the government recognizes, a reasonableness inquiry under the Fourth Amendment would depend on the totality of the circumstances, including "some measure of fit between the search and the desired objective," and the importance of the objective and of the information obtained. Applying that standard, the government has concluded that the NSA program is reasonable and therefore constitutional. I see no meaningful way to test that conclusion without the relevant facts, and the government apparently has concluded that it cannot provide those facts. Further discussion must await resolution of that informational impasse. If the NSA program ever were evaluated by a court, I believe the government's separation-of-powers and Fourth-Amendment arguments would rise or fall together: It is very hard to imagine a court ruling that the President has plenary power to conduct surveillance that violates the Fourth Amendment.

Comments on Possible Legislation

I have been asked to discuss possible legislation that would regulate the NSA surveillance program. I appreciate the request, and I believe that a statute of some kind should be considered. As explained above, in my view the NSA surveillance violates FISA. Even if the President has inherent constitutional authority to do so - an issue on which I have not taken a position - an outright clash between two branches of government is not an appealing prospect for the long term. It therefore makes sense to review potential legislative solutions.

It is somewhat easier to critique legislation than to write it. A few days ago, Senator Specter's staff sent me his draft bill, which I think is an excellent vehicle for debate by informed persons. I am no expert, but I suspect the legislative process here may be long and arduous. The sooner there is something concrete to discuss, the better. Senator Specter's bill is very concrete, and to me that is a virtue, because this is an area in which details matter. All sides should benefit from having something so thoroughly set out. I also recently reviewed Senator DeWine's bill, which takes a slightly different approach. It too is an excellent vehicle for discussion.

At the conceptual level, both bills reflect the idea that FISA should not be scuttled altogether or confined to surveillance of purely domestic (rather than international) communications. Rather, they amend FISA to accommodate, and regulate, the use of new technologies and/or surveillance practices by the Executive Branch. In particular, Senator Specter's bill would authorize the FISC to approve not only individual instances of electronic surveillance - involving a particular target using or about to use particular facilities - but also "electronic surveillance programs." As I understand it, these "programs" essentially consist of criteria governing surveillance that would be applied to many possible targets and facilities by operational personnel. In other words, the programs are the instructions given to the front-line intelligence officers who collect information, as appears to be the case now at the NSA. Senator DeWine's bill would substitute intensive legislative oversight for judicial review of such programs.

Both bills appear responsive to the government's operational justification for the NSA program. The government has explained that the "President authorized the [program] because it offers . . . speed and agility . . . . Among the advantages offered by the [program] compared to FISA is who makes the probable cause determination and how many layers of review will occur before surveillance begins." The government's explanation continues:

Under the [program], professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communications systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. By contrast, because FISA requires the Attorney General to "reasonably determine[]" that "the factual basis for issuance of" a FISA order exists at the time he approves an emergency authorization, see 50 U.S.C. § 1805(f)(2), as a practical matter, it is necessary for NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General to review a matter before even emergency surveillance would begin.

In sum, the government reports, the "relevant distinction between the two methods - and the critical advantage offered by the [NSA surveillance program] compared to FISA - is the greater speed and agility it offers."

It is worth focusing for a moment on Senator Specter's proposal to allow judicial review of surveillance programs. In effect, this approach would treat all standards governing electronic surveillance in the way that minimization procedures are treated under FISA's current provisions. The government would propose, and the FISC would approve, the standards; and the government would apply those standards to particular facts, making judgments in real time. Then, just as the FISC currently may assess compliance with minimization procedures after the fact, and order modifications if necessary at the next renewal, so the FISC would assess all standards governing the surveillance.

Requiring judicial review both before and after the fact will probably add to public confidence and acceptance. In addition, operational personnel within the Executive Branch may well appreciate working with judicial approval. But it may not be acceptable to a legislating majority. In any event, given the range of opinions being expressed today, allowing the NSA surveillance but requiring judicial review may be a reasonable approach, at least as a matter of realpolitik. It is hard for me to know; there are, of course, many possible paradigms that could work.

Requiring judges to review surveillance programs raises some constitutional questions, and I have to say that I am not sure of the answers. First, such judicial review may raise a case-or-controversy question under Article III. There is an argument that it satisfies Article III because something concrete is at stake when the government tries to begin the surveillance, and there is the possibility of a motion to suppress in subsequent litigation. In 1978, the Office of Legal Counsel opined in a letter to Congress that while it was a "difficult question," FISA satisfied Article III. Some, but perhaps not all, of the reasoning in the OLC letter seems applicable to the programmatic judicial review embodied in Senator Specter's bill. In any event, it is an issue to be explored, the OLC letter is a good place to start, and after thinking about it over a long weekend, that is all I can say.

A second issue concerns the Warrant Clause of the Fourth Amendment. Here too, I don't have anything definite to offer. At first glance, Senator Specter's bill may look like it calls for a general warrant, which (by definition) would be unconstitutional. On the other hand, as explained in the first part of my testimony, this is an area in which the Fourth Amendment allows warrantless surveillance under the proper conditions. There is an argument that under Senator Specter's bill, the court's order is not a (general) warrant, but only an authorization for warrantless surveillance that is more likely to be "reasonable" under the Fourth Amendment because it is subject to advance judicial review. I have not studied the question at any length, but I must say that I am instinctively sympathetic to this point of view.

Both of these constitutional questions, and perhaps others, would have to be resolved definitively before any legislation is enacted. For now, it is all I can do to flag them. If, in the end, Article III judicial review of surveillance programs is not permitted, and if there is no desire to create some non-Article III entity like the United States Surveillance Commission, it will be relatively easy to make adjustments, as discussed in more detail below. For now, I will assume that Senator Specter's approach is constitutional.

At the technical level, I confess I don't fully understand all of the details of either Senator Specter's bill or Senator DeWine's bill. This may be a product of the drafters' knowledge and my ignorance of certain facts. If I were legislative counsel, instructed to write a bill allowing the use of FISA surveillance programs (with or without judicial review), I would start with something like what appears on the following page. I must emphasize that this is very tentative - really nothing more than a hurried sketch - and would surely benefit from more extended consideration, particularly by those who know what NSA is doing. I offer it, again, without knowledge of the relevant facts, and without trying to opine on any of the broad policy questions raised here, but merely as a scribe working hastily within the conceptual framework established by others. The draft presents three new provisions of FISA, 50 U.S.C. §§ 1881-1883, and includes optional or alternative language enclosed in double brackets. An explanation of the draft begins on the page immediately following.

50 U.S.C. § 1881. TERRORIST SURVEILLANCE

Notwithstanding any other law, the President [[, through the Attorney General,]] may authorize electronic surveillance for periods of up to 45 days [[90 days]] if -

(a) the electronic surveillance is conducted under specific standards and procedures, approved by the Attorney General, that are reasonably designed to ensure compliance with the following requirements -

(1) the electronic surveillance is conducted only when it cannot with due diligence be conducted under the standards and procedures set forth in sections 1804-1805 and 1842-1843 of this title;

(2) the information acquired by the electronic surveillance is part of an international communication;

(3) a significant purpose of the surveillance is to obtain [[the information sought by the surveillance is]] foreign intelligence information [[as defined in 50 U.S.C. § 1801(e)(1)(A)-(B) and/or concerning a foreign power against which there is in effect a Congressional authorization to use military force]];

(4) with respect to electronic surveillance of information other than dialing, routing, addressing, and signaling information utilized in the processing and transmitting of a communication -

(A) there is probable cause to believe that the communication was sent to or from a foreign power or the agent of a foreign power [[or a person affiliated with a group engaged in international terrorism or activities in preparation therefor]]; and

(B) the minimization procedures with respect such surveillance meet the definition of minimization procedures set forth in section 1801(h) of this title;

(b) promptly [[within 15 days]] after the surveillance is authorized, the Attorney General provides to [[a subset of]] the committees listed in section 1808 of this title, and to the [[presiding judge of the]] court established by section 1803 of this title, the following -

(1) a report setting forth the standards and procedures governing the surveillance, including an explanation of how and why they are reasonably designed to ensure compliance with the requirements of subsection (a) of this section; and

(2) an accounting, reasonably to date, of any related surveillance previously conducted under this subchapter [[including any deviations from the standards and procedures governing the surveillance; the number of communications, communications facilities, and U.S. persons subjected to the surveillance; the types of attributes (such as the number or other identifier) of all U.S. person communications subjected to the surveillance; and a summary of the foreign intelligence information acquired from the surveillance]]; and

(c) the surveillance is conducted in conformity with any orders of the court issued under section 1882 of this title.

50 U.S.C. § 1882. JUDICIAL REVIEW

(a) Upon receipt of the information provided under subsection (b) of section 1881 of this title, the court shall promptly [[within 7 days?]] assess it and issue an order approving the standards and procedures governing the surveillance, or directing the Attorney General to make such modifications to them or to take such other actions as are necessary to satisfy section 1881 [[and the Fourth Amendment to the U.S. Constitution]].

(b) An order issued by the court under this section requiring the Attorney General to make modifications or take other actions shall be accompanied by a written statement of reasons and subject to further review as would an order denying an application under section 1805 of this title.

(c) With respect to any electronic surveillance determined to have been conducted in violation of this subchapter [[or the Fourth Amendment to the U.S. Constitution]], no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

50 U.S.C. § 1883. ASSISTANCE FROM THIRD PARTIES AND DEFINITIONS

(a) With respect to electronic surveillance authorized by section 1881 of this title, the Attorney General or his designee may direct a communication common carrier or other specified party to -

(1) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier or other specified party for furnishing such aid.

(b) A party who, in good faith, complies with a direction under this section shall not be liable to any other person for such compliance.

(c) Unless otherwise indicated, terms used in this subchapter shall have the same meanings as in section 1801 of this title.

(d) For purposes of this subchapter, the term "international communication" means a communication involving at least one party located inside the United States and at least one party located outside the United States.

[[(e) As used in section 1881 of this title, the word "affiliated" means . . .]]

As noted, the foregoing draft legislation takes its policy and constitutional cues from Senator Specter's bill and, to a lesser extent, from Senator DeWine's bill. Thus, for example, it does not simply narrow the definition of "electronic surveillance" in FISA to exclude international communications. It does include judicial review, but that review can be eliminated by making three minor changes specified below. The draft is meant to be modular; elements can be added or removed without changing its basic structure.

The draft would allow the President (or, as an alternative, the Attorney General) to authorize electronic surveillance - subject to judicial review if desired - for renewable periods of 45 days (lines 3-4). The surveillance would be authorized if, and only if, it met each of the conditions specified in proposed 50 U.S.C. § 1881. There are three main groups of conditions. First, the surveillance would have to satisfy certain substantive requirements set out in proposed Section 1881(a), such as a requirement that it be conducted under specific procedures reasonably designed to ensure that the contents of a communication cannot be acquired without probable cause. Second, the government would have to provide certain information about the surveillance to the Congressional Intelligence Committees and the Foreign Intelligence Surveillance Court (FISC). Third and finally (if desired as a policy matter), the surveillance would have to be conducted in accord with any orders of the FISC.

I. Substantive Requirements.

The draft contemplates that the Attorney General, or his subordinates, in consultation with the relevant operational agency (e.g., NSA), would draft protocols governing the surveillance. These protocols would serve as a kind of instruction manual to the persons actually collecting the information; the government has indicated that such instruction manuals already exist. The protocols would have to set out "specific standards and procedures" governing the surveillance that are "reasonably designed to ensure compliance" with the general requirements in the draft legislation (lines 6-8). The use of the phrase "specific standards and procedures" is meant to parallel the language elsewhere in FISA describing minimization procedures, which are defined as "specific procedures" that meet the general standards in current 50 U.S.C. § 1801(h). FISA's legislative history provides:

The definition begins by stating that the minimization procedures must be specific procedures. This is intended to demonstrate that the definition is not itself a statement of the minimization procedures but rather a general statement of principle which will be given content by the specific procedures which will govern the actual surveillances. It is also intended to suggest that the actual procedures be as specific as practicable in light of the technique of the surveillance and its purposes.

The same idea motivates the use of the phrase "specific standards and procedures" here. The procedures adopted under proposed Section 1881 need only be "reasonably designed" to satisfy the standards in the draft. Perfection is not attainable; some overruns or errors are inevitable. But the procedures would have to be written reasonably to minimize the risk of error.

There is also an analogy to current 50 U.S.C. § 1802, under which the Attorney General may authorize electronic surveillance without a court order if he certifies in writing and under oath that certain conditions are satisfied (generally, that the facility being surveilled is used exclusively by foreign powers, and that there is no substantial likelihood of acquiring the communications of a U.S. person). The conditions in Section 1802 are narrower than those in the draft, but the basic idea is the same, and Section 1802 provides expressly that the surveillance "may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him." In any given case, if the facts require detailed procedures to ensure compliance with Section 1802's general requirements, then the minimization procedures must contain them. The same is true here.

The procedures approved by the Attorney General would have to be "reasonably designed" to "ensure compliance" with the specific requirements that are described in detail below. The first three of those requirements are that the surveillance be conducted only when (A) normal FISA procedures cannot be used; (B) the communication being monitored is international; and (C) the government has a significant purpose to obtain foreign intelligence information (or some subset of foreign intelligence information).

A. Inability to Use Normal FISA Procedures.

The first substantive condition, set out in proposed Section 1881(a)(1), is that the surveillance be conducted only when it "cannot with due diligence be conducted" under FISA's ordinary procedures (lines 10-12). This language is borrowed from current 50 U.S.C. § 1805(f)(1), which allows the Attorney General to authorize electronic surveillance without a court order where "an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained" (emphasis added). The idea is that Section 1881 surveillance should not be conducted except where it must be, so that the exception does not swallow the rule. If that standard is deemed too strict, an alternative - e.g., "without substantially hindering the surveillance" - could be used. One specific standard that might be used to ensure adherence to the requirement would be a rule barring continuous surveillance of the same communications facility (e.g., a telephone line) for more than 72 hours (or perhaps longer), on the theory that if the surveillance endures that long, there is time at least to get an emergency FISA. (One drawback to this approach is that, if the substantive standards in the draft are reduced so that they are vastly lower than those in the rest of FISA, it may be that surveillance on relatively weak evidence may endure for a very long time. There are, of course, legislative and sub-legislative ways to deal with that problem.)

B. Limited to International Communications.

The second condition (lines 14-15) is that the information acquired by the surveillance be part of an international communication. This limitation is not essential, but reflects the scope of the NSA surveillance program as it has been described publicly. As noted in the first part of my testimony, limiting surveillance to international communications may affect the Fourth Amendment analysis. The definition of "international" is set out in proposed Section 1883(d) of the draft (lines 101-103). A full discussion of the application of such a definition is beyond the scope of this testimony in this forum. The government has confirmed that, under the NSA program, "[t]here are procedures in place to avoid the interception of domestic calls."

C. Foreign Intelligence Information.

The third condition (lines 17-20) concerns the purpose of the surveillance. Here I have borrowed from the current law. If surveillance is to be allowed under this new statute, I see no basis for rebuilding a wall between intelligence and law enforcement officials. We have been down that road before. If "foreign intelligence information" is limited in either of the two ways set out in the language in double brackets, as discussed in the next two paragraphs, the better phrasing might be that "the information sought by the surveillance is . . . ."

The first limit in double brackets would restrict the foreign intelligence information being sought to that concerning "attack or other grave hostile acts . . . [or] sabotage or international terrorism," rather than "clandestine intelligence activities" and "affirmative" foreign intelligence. Does the government need to use the NSA surveillance program against espionage? Should it be permitted to? I don't know, but the draft flags the issue. Obviously, any other limits that are desired could be inserted here.

The second limit in double brackets would restrict the foreign intelligence information being sought to that concerning foreign powers against which Congress has authorized the use of military force. I added this possibility principally because the Executive Branch has relied so heavily on the September 2001 AUMF in defending the NSA surveillance program. This condition puts substantially more power in the hands of Congress because, if no authorization is enacted, no surveillance may occur. I doubt the Executive Branch would accept this limit, and I acknowledge that it has several drawbacks. First, of course, it depends on Congress enacting an authorization; Congress acted quickly after September 11, but it might not be able to do so after a decapitation strike - a situation in which aggressive electronic surveillance might be most needed. Second, Congress may want to authorize the use of military force before it knows exactly who is responsible for an attack, leaving it to the President to find the enemy; ambiguity in the authorization would yield ambiguity under the draft.

D. Pen-Trap Surveillance and Surveillance of Contents.

1. Pen-Trap Surveillance. It would be possible to allow the use of a pen register and trap-and-trace device (pen-trap surveillance) under procedures that reasonably ensure compliance with the foregoing three conditions alone - (A) inability to use ordinary FISA procedures; (B) surveillance of international communications only; and (C) a purpose to obtain foreign intelligence information. Pen-trap surveillance involves the acquisition of dialing, routing, addressing, and signaling information utilized in the processing and transmitting of a communication. An example of such routing and addressing information is a telephone number. Pen-trap surveillance does not, however, involve the acquisition of what Title III, the law-enforcement electronic surveillance statute, refers to as "contents" - i.e., "any information concerning the substance, purport, or meaning of [a] communication." An example of contents is the words spoken in a telephone conversation. Under current law, the FISC must approve pen-trap surveillance for individual facilities (e.g., telephone numbers). By contrast, under the draft, the facilities would be selected by operational personnel in accord with the standards and rules that govern the surveillance program.

2. Middle Ground. One other possibility bears mentioning. The line between contents and routing and addressing information is not always bright and clear, although it is deeply embedded in the law of electronic surveillance. It would be a big task, but if necessary for this legislation, Congress could attempt to define more precisely which attributes of a communication are and are not "contents." (For this project, knowing what NSA can do technically, and hopes to be able to do technically in the near future, would be helpful, but the law would have to be written in a way that does not reveal that. As noted earlier, I have no classified information on the NSA program.)

I can imagine Congress creating by statute, and the courts endorsing, a third category of information, between traditi