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).[1] 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).[2] However, I was not read into the NSA surveillance program, and I have no classified information concerning it.[3]

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.[4] 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[5]; (2) FISA's "exclusivity provision"[6] prohibits such surveillance except under the "procedures" in FISA; (3) the September 2001 Authorization to Use Military Force (AUMF),[7] as interpreted by the Supreme Court in *Hamdi* v. *Rumsfeld*,[8] 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.[9] 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.[10] 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."[11] He also said that FISA "requires a court order before engaging in this kind of surveillance."[12] 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."[13] The definition is even broader as applied to the targeting of United States persons – *e.g.*, a citizen or green-card holder.[14]

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."[15] It "assume[s] . . . that the activities described by the President constitute 'electronic surveillance' as defined by FISA,"[16] although it also argues that the definition produces some anomalies in light of changing technology and other factors.[17] 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.[18] 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."[19] 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.[20]

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.[21]

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).'"[22]

Indeed, FISA repealed a provision of Title III disclaiming any intent to limit the "constitutional power of the President" in this area.[23] This disclaimer provision, the Supreme Court held in 1972, "simply left presidential powers where it found them."[24] 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."[25] 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."[26] 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.[27]

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."[28] 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."[29] 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.[30] 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,[31] courts likely would overcome their normal aversion, and find an

implied repeal (or amendment) of the latter by the former.[32] An ambiguous new statute, however, would be read not to authorize electronic surveillance in order to avoid a conflict with the exclusivity provision.[33] 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."[34] 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]."[35] 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.'"[36]

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.[37] 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."[38] 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.[39] 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."[40] 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.[41] 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."[42] 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."[43]

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.[44] 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.[45]

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.[46] 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."[47] 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"[48] – as well as the statute's rules permitting electronic surveillance in certain circumstances without the FISC's approval.[49] 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.[50]

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."[51] 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."[52] 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),[53] a joint resolution passed by Congress and signed by the President shortly after the September 11, 2001, attacks.[54] In *Hamdi* v. *Rumsfeld*, the Supreme Court concluded that the AUMF authorized the use of military detention.[55] 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."[56]

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;[57] electronic surveillance of telegraph signals was apparently conducted as early as the Civil War.[58] DOJ's whitepaper traces this history in detail,[59] and the NSA has published an informative study on the history of signals intelligence in war that makes similar assertions.[60] 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.[61]

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.[62] The Patriot Act, of course, substantially amended FISA to aid the government's efforts against terrorism.[63] 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."[64] 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.[65]

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.[66]

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.[67] 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."[68] 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.[69] 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?[70] 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."[71] 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,[72] every court of appeals to decide that issue had upheld the President's authority.[73] 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.[74] The DOJ whitepaper contains an extensive discussion of these points that I am more or less prepared to accept for present purposes.[75]

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."[76] The government accepts this.[77] 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?[78] 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).[79] 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."[80] As a functional matter, the question is whether one branch has unduly "impair[ed] another in the performance of its constitutional duties."[81] DOJ appears to agree that these are the relevant tests.[82]

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.[83] 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."[84] The Court has said that under this clause Congress "exercises a power of precedence over . . . Executive authority."[85] 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."[86] 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.[87]

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."[88] 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.[89] 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,[90] Congress in December 2005 passed, and the President signed, a law that would ban the torture of such detainees.[91] 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."[92] 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.[93] In such instances, the President apparently believes, his power to torture is plenary.[94]

All of these real and hypothetical examples illustrate what Professor Corwin famously called the Constitution's "invitation to struggle" for dominance in foreign affairs.[95] 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.[96] The Constitution is not a suicide pact.[97]

The second question concerns the reasons for eschewing the use of FISA in obtaining the information.[98] For example, if FISA did not contain an emergency exception,[99] 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,[100] 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*,[101] 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."[102] The Court rejected the argument that, despite this general principle, "mailed letters are somehow different."[103] 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.[104]

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.'"[105] In other locations, the whitepaper refers to a "reasonable belief" or its equivalent.[106] Translated into Fourth Amendment terms, this could be viewed as a reference to "reasonable suspicion," which of course is something less than probable cause.[107] 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.'"[108] 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.[109]

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.[110] 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.[111] 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.[112] 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.[113] 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."[114] 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.[115]

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."[116]

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.[117] Then, just as the FISC currently may assess compliance with minimization procedures after the fact,[118] 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.[119] 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.[120] 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.[121] 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,[122] 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.[123] 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.[124] 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.[125]

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).[126] 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."[127] 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.[128] The definition of "international" is set out in proposed Section 1883(d) of the draft (lines 101-103).[129] 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."[130]

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.[131] 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.[132] 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."[133] 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.[134] 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 traditional routing and addressing information and full contents, that might be available to the government on a showing of something like reasonable suspicion. Congress might decide – and the courts might (or might not) concur – that such information is entitled to intermediate protection. I don't mean to suggest that this would be constitutional, or even helpful; I say only that it might be worth considering.

3. Contents. To acquire the "contents" of a communication, or information that is not subject to pen-trap surveillance, the government would have to satisfy two additional substantive requirements set out in the draft (lines 26-32). First, it would need to have probable cause that the communication was sent to or from a foreign power or the agent of a foreign power. Persons conducting the surveillance would follow procedures that require them to make probable-cause determinations in particular cases. Operationally, it might be very similar to current NSA practice as it has been described by the government.[135]

The language in double brackets that is associated with the probable-cause requirement would extend not only to agents of foreign powers, but also to persons "affiliated" with an international terrorist group. I do not know what the word "affiliated" would mean in this context, but the government has used the term in describing the scope of the NSA surveillance program. In particular, the government has said that the program requires "probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization."[136]

Some, but perhaps not all, of "affiliation" already fits within the definitions of "foreign power" and "agent of a foreign power" in current 50 U.S.C. § 1801(a) and (b). Indeed, the government has at least once effectively stated that the NSA program, including the concept of "affiliation," does not exceed FISA's current definitions. In response to a question about my testimony before this Committee in 2002, Attorney General Gonzales wrote that the NSA surveillance program "involves the interception of communications only when there is probable cause ('reasonable grounds to believe') that at least one party to the communication is an agent of a foreign power (al Qaeda or an affiliated terrorist organization)."[137] If that is so, then FISA's current definitions will suffice, and the word "affiliated" need not be added to the draft. If broader definitions are desired, then affiliation or some other concept could be used, as long as it is defined properly. The draft leaves a place to define "affiliated" in line 105. Of course it

would also be possible to limit the definitions – *e.g.*, to allow surveillance only where one party to the communication is an agent of a foreign power involved in terrorism or related activities, rather than espionage or other kinds of activities. It is a policy choice.

The second condition required for the surveillance of "contents" would be the use of minimization procedures. As discussed above, minimization procedures govern the acquisition, retention, and dissemination of information under FISA, and fundamentally must balance the government's need to obtain foreign intelligence information against the privacy interests of U.S. persons.[138] They are a conventional part of electronic surveillance, and the government has stated that there are minimization procedures already in effect in the NSA surveillance program. If the scope of proposed Section 1881(c) is limited to a subset of foreign intelligence information (lines 18-20), then the minimization procedures as used here would have to contain a similar limit.

II. Procedural Conditions.

The draft requires the Attorney General to provide information about the surveillance to Congress and to the FISC. (Double bracketed language allows for use of subsets of those entities.) Promptly after the surveillance is authorized, the Attorney General would have to provide two things. First, under proposed Section 1881(b)(1) (line 38), "a report setting forth the standards and procedures governing the surveillance." This report likely would contain the instructions provided to the operational personnel at NSA or another agency, as well as a memorandum explaining why the instructions are in fact "reasonably designed to ensure compliance with" the statutory requirements and (as necessary beyond the statutory discussion) the Fourth Amendment.

The Attorney General also would have to provide a reasonably timely "accounting" of "any related surveillance previously conducted," as set out in proposed Section 1881(b)(2) (lines 38-43). When surveillance is commenced, of course, there would be no accounting. Upon renewal, however, the Attorney General would describe the surveillance previously conducted; as renewals mounted, the accounting could incorporate by reference the descriptions submitted previously. As a practical matter, therefore, after the initial surveillance authorization, the Attorney General at each renewal would be reporting on approximately the previous 45 days of surveillance.

The language in double brackets (lines 43-48) sets out with particularity the kind of information that could be included in the accounting. Examples include requiring the Attorney General to provide information about 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 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. Whether to include that level of specificity in the statute is a policy judgment. One alternative is simply to require the Attorney General to keep the Committees and the Court "fully informed," which is the traditional oversight standard.[139] In this new context, however, more precision in the statute may be better.

The information provided would be used by the FISC to inform its ongoing review of the surveillance program, and in particular the question of whether the specific standards and procedures are indeed "reasonably designed" to satisfy legal requirements. The information would be used by Congress in keeping with the traditions of intelligence oversight. Both the FISC and the Congressional Committees would, of course, maintain the information under proper security procedures.

III. Conforming to Court Orders and Judicial Review.

Finally, under proposed Section 1881(c), the surveillance would have to be conducted in conformity with any orders of the FISC. As the draft is written, the surveillance would be authorized, and could be commenced, without judicial approval, as is the case with emergency FISA surveillance.[140] But the FISC would be required to review and approve (or disapprove) the surveillance within a fixed time period. If the government changed the standards and procedures governing the surveillance before 45 days expire, it would need promptly to provide the new procedures to the FISC (and to Congress).

Proposed Section 1882 (lines 48-70) explains how the FISC would conduct its review. The court would have a short period of time to consider the government's report and either (1) approve the standards and procedures proposed by the government, or (2) order modifications to them. If modifications were ordered, the government would be entitled to appeal. If surveillance were found to violate the statute (or the Fourth Amendment), the information obtained from it would be suppressed and generally would not be available for use (except where death or serious bodily harm may result).

If Congress determines that judicial review is unconstitutional, or otherwise inappropriate, the draft could be changed to accommodate that. To eliminate the FISC's role, three changes would need to be made:

- delete the deference to the FISC in proposed Section 1881(b), lines 35-36 (this could be retained if the FISC should be kept informed even if it does not review the program);
- delete proposed 50 U.S.C. § 1881(c) in its entirety, lines 50-51; and
- delete proposed Section 1882 in its entirety, lines 52-75.

IV. Miscellaneous Provisions.

Finally, proposed Section 1883 of the legislation has fairly standard language allowing the Attorney General to direct assistance from third parties, insulating those third parties from liability if they obey the Attorney General, and defining some of the terms used in the draft. There might need to be additional provisions, mirroring those in 50 U.S.C. § 1806, governing use and disclosure of information obtained from the surveillance. Those should not be too hard to draft.

## Conclusion

Thank you again for the opportunity to testify. I repeat that my analysis, particularly with respect to possible legislation, is hindered by my ignorance, and that I have not tried to stake out strong positions on most of the policy issues. Particularly in the absence of facts, I feel more comfortable proceeding with extreme caution.

## Notes

[1] See James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, New York Times, at A1 (Dec. 16, 2005); President's Weekly Radio Address (Dec. 17, 2006) (available at http://www.whitehouse.gov/news/releases/2005/12/20051217.html).

[2] The views expressed in this testimony are solely my own, not those of any current or former employer.

[3] This testimony has been cleared by DOJ under 28 C.F.R. § 17.18.

[4] I have used the notes, rather than text, for the most arcane or uncertain elements of the analysis.

[5] 50 U.S.C. §§ 1801 et seq. FISA's definition of "electronic surveillance" appears in 50 U.S.C. § 1801(f).

[6] 18 U.S.C. § 2511(2)(f).

[7] Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001).

[8] 542 U.S. 507 (2004).

[9] Letter from Assistant Attorney General William E. Moschella, U.S. Department of Justice, to the Chairs and Ranking Members of the House and Senate Intelligence Committees, at 1 (Dec. 22, 2005) (available at http://www.nationalreview.com/pdf/12%2022%2005%20NSA%20letter.pdf) (hereinafter DOJ 12-22-05 letter); Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006) (available at http://rawstory.com/other/justicerawstory.pdf) (hereinafter DOJ Whitepaper).

[10] See DOJ Whitepaper at 35-36 & n.21.

[11] Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) (available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html) (hereinafter 12-19-05 briefing transcript). See also DOJ 12-22-05 Letter at 1 ("As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization").

[12] 12-19-05 briefing transcript. Strictly speaking, the most that could be said is that FISA generally requires a court order; the statute allows for electronic surveillance without a court order in certain situations. See note 49, *infra*.

[13] 50 U.S.C. § 1801(f)(2). This provision of FISA defines "electronic surveillance" to include:

> the acquisition by an electronic, mechanical, or other surveillance device of 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, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code.

This provision applies to wire communications, such as corded telephone calls while they are traveling on a wire or cable, regardless of the citizenship or immigration status of the persons involved, as long as either the sender or recipient of the communication is in the United States, and neither sender nor recipient consents to the wiretap. It does not apply to radio communications and it excludes a narrow band of communications of computer trespassers, who are likewise unprotected by Title III, the 1968 wiretapping law applicable to ordinary criminal investigations, 18 U.S.C. §§ 2510-2522.

Under 50 U.S.C. § 1801(f)(1), "electronic surveillance" is also defined to include

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

This is the principal provision applicable to wiretaps of United States persons – *e.g.*, U.S. citizens or permanent resident aliens – who are inside the United States. In essence, it applies whenever the government tries to overhear or record a telephone call or other similar communication to or from such a person, if (and only if) a warrant would be necessary for the same wiretap conducted for ordinary law enforcement purposes under Title III or a similar law. The subsection applies equally to domestic and international communications made by U.S. persons in the United States.

[14] 50 U.S.C. § 1801(f)(1). The term "United States person" is defined in 50 U.S.C. § 1801(i).

[15] DOJ Whitepaper at 5; see *id.* at 1, 13 n.4, 40.

[16] *Id.* at 17 n.5. In a speech given on January 24, 2006, the Attorney General explained that, "because I cannot discuss operational details, I'm going to assume here that intercepts of al Qaeda communications under the terrorist surveillance program fall within the definition of 'electronic surveillance' in FISA." Prepared Remarks for Attorney General Alberto Gonzales, at the Georgetown University Law Center (Jan. 24, 2006) (available at http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html) (hereinafter Georgetown Prepared Remarks). There is also some discussion in the Whitepaper of how FISA did not intend to regulate certain NSA surveillance activities. See DOJ Whitepaper at 18-19 & n.6 (discussing the first clause of 18 U.S.C. § 2511(2)(f) and citations of the Church Committee Report in FISA's legislative history).

[17] See DOJ Whitepaper at 18-19 & n.6, 35 & n.20.

[18] If NSA was not engaged in "electronic surveillance," then the analysis would be quite different because the surveillance program probably would not be governed by any statute, but only by Executive Order 12333 and the Fourth Amendment. Under the first clause of the exclusivity provision, the government may use any "means other than electronic surveillance as defined in FISA" to acquire "foreign intelligence information from international or foreign communications" without regard to the law-enforcement surveillance statutes or (obviously) FISA. 18 U.S.C. § 2511(2)(f).

[19] 18 U.S.C. § 2511(2)(f) (emphasis added). Section 2511(2)(f) now provides as follows:

> Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

Chapter 121 of Title 18 is the Stored Communications Act, 18 U.S.C. §§ 2701-2712, and Chapter 206 contains the criminal pen-trap surveillance statutes, 18 U.S.C. §§ 3121-3127. Section 705 of the Communications Act of 1934 is codified at 47 U.S.C. § 605. For a discussion of the legislation adding the reference to the Stored Communications Act, and other legislation amending the exclusivity provision, see note 30, *infra*.

[20] *Id.*

[21] H.R. Rep. No. 95-1283, Part I, at 101. See also S. Rep. No. 95-604, at 6, 63, 64 (FISA "puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in [Title III and FISA]"); S. Rep. No. 95-701, at 71 (same).

[22] H.R. Rep. No. 95-1720, at 35; see S. Rep. No. 95-604, at 16 & n.28.

[23] Section 201 of FISA repealed 18 U.S.C. § 2511(3), which provided: "Nothing contained in [Title III] or in section 605 of the Communications Act of 1934 shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power."

[24] *United States* v. *United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 303 (1972) (*Keith*).

[25] H.R. Rep. No. 95-1283, Part I, at 101-102. See S. Rep. No. 95-604, at 17 ("Most importantly, the disclaimer in 18 U.S.C. § 2511(3) is replaced by provisions that assure that [FISA], together with [Title III], will be the *exclusive* means by which electronic surveillance covered by [FISA], and the interception of wire and oral communications, may be conducted" (italics in original)). As the Seventh Circuit has explained, "much concern was expressed in the debates about the constitutionality as well as the prudence of Congress's displacing by legislation the President's implicit authority under Article II to protect the nation's security against intrigues by foreign powers. The debate was resolved in favor of the proposed legislation." *United States* v. *Torres*, 751 F.2d 875, 882 (7th Cir. 1985) (citations omitted); cf. *United States* v. *Biasucci*, 786 F.2d 504, 508 n.4 (2d Cir. 1986). The courts of appeals have not had much occasion to discuss the effect of the exclusivity provision on foreign intelligence investigations, although they have ruled on its application to ordinary criminal investigations. See, *e.g.*, *United States* v. *Falls*, 34 F.3d 674 (8th Cir. 1994) (joining several other circuits in holding that silent television surveillance, which is "electronic surveillance" under FISA but is not the "intercept[ion of] wire, oral, or electronic communications" under Title III, is not prohibited by the exclusivity provision in the context of ordinary criminal investigations because FISA does not limit investigative activity in ordinary criminal cases). These decisions are discussed further in note 50, *infra*.

[26] S. Rep. No. 95-604, at 8.

[27] See DOJ Whitepaper at 18-20. The whitepaper acknowledges that "Congress intended FISA to exert whatever power Congress constitutionally had over the subject matter to restrict foreign intelligence surveillance and to leave the President solely with whatever inherent constitutional authority he might be able to invoke against Congress's express wishes." *Id.* at 19. In other words, as the whitepaper summarizes, Congress "enacted a regime intended to supplant the President's reliance on his own constitutional authority." *Id.* at 20.

[28] S. Rep. No. 95-604, at 63; see S. Rep. No. 95-701, at 71 (same).

[29] S. Rep. No. 95-701, at 71. Cf. H.R. Rep. No. 95-1720, at 35 (discussion of statutory and constitutional authority indicating that the word "statutory" was removed from the exclusivity provision to ensure that it would be read to limit the President's constitutional power, without suggesting that the provision applies only to the President's constitutional power).

[30] The Stored Communications Act, now codified as chapter 121 of Title 18 (18 U.S.C. §§ 2701-2712), was part of the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986). Section 101(b)(3)

of ECPA amended the exclusivity provision to refer explicitly to the Stored Communications Act. See S. Rep. No. 99-541, at 18.

Here is a history of amendments to the exclusivity provision. As enacted by Section 201(b) of FISA, Pub. L. 95-511, 18 U.S.C. § 2511(2)(f) provided as follows:

> Nothing contained in this chapter, or section 605 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Since then, Section 2511(2)(f) has been amended three times. First, Section 6(b)(2)(B) of the Cable Communications Policy Act, Pub. L. 98-549, replaced "section 605" with "section 705" in referring to the Communications Act of 1934. Second, in addition to making the changes noted above, Section 101(b)(3) of ECPA also added the phrase "or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing" in place of the word "by" after the reference to "international or foreign communications." Third, Section 204 of the USA Patriot Act, Pub. L. 107-56, added references to "chapter 206" and substituted "wire, oral, and electronic" for "wire and oral" at the end of the provision, in keeping with amendments made to other provisions of Title III by Section 101(c)(1)(A) of ECPA. The text of the exclusivity provision in its current form – citing FISA, Title III, and the Stored Communications Act – is set out at note 19, *supra*. The Patriot Act's amendment to the exclusivity provision is discussed further in note 65, *infra*.

[31] *Branch* v. *Smith*, 538 U.S. 254, 273 (2003) (plurality opinion).

[32] See, *e.g.*, *United States* v. *Borden Co.*, 308 U.S. 188, 198 (1939).

[33] See generally, *e.g.*, *FDA* v. *Brown & Williamson*, 529 U.S. 120, 132-133 (2000); cf. *Pasquantino* v. *United States*, 125 S. Ct. 1766, 1777 (2005).

[34] DOJ Whitepaper at 20.

[35] *Id.* at 22 (italics in original).

[36] *Id.* at 26 (quoting *Fletcher* v. *Peck*, 10 U.S. (6 Cranch) 87, 135 (1810)).

[37] *Lockhart* v. *United States*, 126 S. Ct. 699, 701 (2005) (quoting *Marcello* v. *Bonds*, 349 U.S. 302, 310 (1955)).

[38] *Id.* at 703 (Scalia, J., concurring).

[39] S. Rep. No. 94-755.

[40] At least for purposes of this argument, the government does seem to acknowledge a preclusive effect with respect to other statutes, because its argument is that "FISA permits an exception" to the acknowledged rule set out in the exclusivity provision. DOJ 12-22-05 Letter at 3.

[41] *Id.*

[42] 50 U.S.C. § 1809 (emphasis added); see 50 U.S.C. § 1810 (civil liability). Section 1809 provides in pertinent part as follows:

> (a) Prohibited activities.

A person is guilty of an offense if he intentionally –

(1) engages in electronic surveillance under color of law except as authorized by statute;

* * * *

(b) Defense.

It is a defense to prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

[43] DOJ Whitepaper at 20 (italics in original).

[44] FISA's definition of "electronic surveillance," in 1978 and today, includes essentially all of what Title III defines as the "intercept[ion of] wire, oral, or electronic communications," as well as some additional activity. Compare 50 U.S.C. § 1801(f) (FISA's definition of "electronic surveillance"), with 18 U.S.C. § 2510 (definition of corresponding terms in Title III).

[45] H.R. Rep. No. 95-1283, Part I, at 96. The Senate Reports on FISA explained that the penalty provision made it "a criminal offense to engage in electronic surveillance except as otherwise specifically provided in [Title III] and [FISA]." S. Rep. No. 95-701, at 68; S. Rep. No. 95-604, at 61. However, the version of the penalty provision at issue in those reports did not contain an exemption for surveillance "authorized by statute." See S. Rep. No. 95-701, at 75; S. Rep. No. 95-604, at 67-68. In adopting the House version of the penalty provision, the Conference Committee Report does not suggest that Congress was incorporating into FISA's procedures an exception for surveillance conducted under statutes other than FISA and Title III. See H.R. Rep. No. 95-1720, at 33. When Congress enacted FISA's physical search provisions in 1994, it established essentially identical penalty provisions. 50 U.S.C. § 1827. The legislative history of the physical search provisions explains that "[o]ne of the important purposes of [the physical search provisions] is to afford security to intelligence personnel so that if they act in accordance with the statute, they will be insulated from liability." S. Rep. No. 103-296, at 73 (emphasis added). There is no exclusivity provision with respect to physical searches, and so the argument that the penalty and exclusivity provisions should be read together does not apply to the physical search penalty provision.

It is worth noting that even if FISA's penalty provision were read to incorporate all other surveillance statutes, and so to shield individuals from prosecution, it would not necessarily authorize an exception to the exclusivity provision. Governmental conduct may be forbidden without being criminalized. But cf. discussion in note 46, *infra*.

[46] H.R. Rep. No. 95-1283, Part I, at 100 n.54. In its entirety, the footnote reads as follows (citation omitted):

> As noted earlier [page 96 of the report], the use of pen registers and similar devices for law enforcement purposes is not covered by [Title III] or this Act and [the exclusivity provision] is not intended to prohibit it. Rather, because of the criminal defense provision of [FISA's penalty provision, 50 U.S.C. § 1809(b)(1)], the 'procedures' referred to in [the exclusivity provision] include acquiring a court order for such activity. It is the Committee's intent that neither this [exclusivity provision] nor any other provision of the legislation have any effect on the holding in *United States* v. *New York Telephone* that rule 41 of the Federal Rules of Criminal Procedure empowers federal judges to authorize the installation of pen registers for law enforcement purposes.

As far as I know, this footnote has not been cited in the government's public materials on the NSA surveillance. Cf. DOJ Whitepaper at 23 & n.8. In my view, however, it is the best support for the government's position, and so I address it here at some length.

The footnote makes sense only when viewed in context. It is part of a technical discussion of the effect of the exclusivity provision on criminal pen-trap surveillance. When FISA was enacted in 1978, pen-trap surveillance was (and still is) "electronic surveillance" under FISA, but was not authorized by Title III (or by FISA when conducted for ordinary criminal law enforcement purposes). See H.R. Rep. No. 95-1283, Part I, at 51. Instead, criminal pen-trap surveillance was conducted under court order issued pursuant to Federal Rule of Criminal Procedure 41, like an ordinary criminal search warrant. See *id.* at 96 n.51 & 100 n.54 (citing *United States* v. *New York Tel. Co.*, 434 U.S. 159 (1977)). As such, it might have been deemed forbidden by the exclusivity provision.

Congress seems to have adopted the affirmative defense in FISA's penalty provision at least in part to ensure that law enforcement officials could conduct court-authorized criminal pen-trap surveillance without fear of prosecution: "Since certain technical activities – such as the use of a pen register – fall within the definition of electronic surveillance under [FISA], but not within the definition of wire or oral communications under [Title III], [FISA] provides an affirmative defense to a law enforcement or investigative officer who engages in such an activity for law enforcement purposes in the course of his official duties, pursuant to a search warrant or court order." H.R. Rep. No. 95-1283, Part I, at 96. Today, Chapter 206 of Title 18 separately authorizes criminal pen-trap surveillance (18 U.S.C. §§ 3121-3127), Title III contains an exception for pen-trap surveillance (18 U.S.C. § 2511(2)(h)(i)), and FISA separately authorizes foreign intelligence pen-trap surveillance (50 U.S.C. §§ 1841-1846). The judicial decisions cited in note 50, *infra*, have held that FISA does not preclude "electronic surveillance" conducted for ordinary law-enforcement purposes.

[47] 50 U.S.C. § 1809(b). The text of Section 1809 is set out at note 42, *supra*. See H.R. Rep. No. 95-1283, Part I, at 11 (substantially similar version of 50 U.S.C. § 1809 in the version of FISA discussed in the House Report).

[48] 50 U.S.C. § 1803(a) (emphasis added). See 50 U.S.C. §§ 1804 and 1805.

[49] There are four situations in which electronic surveillance may be conducted without advance approval from the FISC: (1) surveillance of communications systems used exclusively by foreign powers where there is no substantial likelihood of acquiring a U.S. person's communications (50 U.S.C. § 1802); (2) emergencies (50 U.S.C. § 1805(f)); (3) training and testing (50 U.S.C. § 1805(g)); and (4) for 15 days following a declaration of war by Congress (50 U.S.C. § 1811). This wartime provision is discussed in more detail at text and note 67, *infra*.

[50] In a series of decisions beginning in 1984, the federal courts of appeals confronted the validity of silent television surveillance approved by court order in criminal investigations. See *Falls*, 34 F.3d at 679-680 (citing cases); note 25, *supra*. Like criminal pen-trap surveillance (see note 46, *supra*), such television surveillance was "electronic surveillance" as defined by FISA but was not authorized by Title III (or by FISA). The courts upheld the surveillance – not on the theory the government advances now, but instead because, as Judge Posner put it, the exclusivity provision means only "that the Foreign Intelligence Surveillance Act is intended to be exclusive in its domain and Title III in its." *Torres*, 751 F.2d at 881; see S. Rep. No. 95-604, at 63-64. In other words, the courts held that FISA simply exerts no preclusive effect on ordinary law-enforcement surveillance, not that it incorporates or allows an "exception" for surveillance conducted under law-enforcement statutes or rules.

To be sure, it is easy to overstate the significance of the fact that these decisions did not adopt the government's current argument. For example, although *Torres* was a government appeal (presumably approved by the Solicitor General), the government apparently did not advance the argument on which it now relies, so the court apparently had no occasion to review it. However, it is worth noting that the Solicitor General adopted and repeated the *Torres* court's interpretation of the exclusivity provision in his brief in opposition to a certiorari petition filed in connection with the case. See *Rodriguez* v. *United States*, No. 86-5987, Brief for the United States in Opposition at __, cert. denied, 480 U.S. 908 (1987) (brief in opposition available at http://www.usdoj.gov/osg/briefs/1986/sg860179.txt). (The significance of that adoption by the Solicitor General also can be overstated, of course, because a brief in opposition generally is not the best place to advance a novel legal argument not considered by the court below.)

In any event, these court decisions also make clear that the government's statutory theory need not be adopted in order to preserve the legality of criminal pen-trap surveillance (or any other law-enforcement investigative activity that is "electronic surveillance" under FISA but is not affirmatively authorized under Title III).

See DOJ Whitepaper at 22; note 46, *supra*. There are two ways to read *Torres* and its progeny, either of which will suffice. First, they can be read to hold that FISA exerts no preclusive effect on law enforcement surveillance authorities (*e.g.*, statutes or rules), and correspondingly that Title III exerts no such effect on foreign intelligence authorities. On this approach, the inquiry turns on the nature of the statute or other authority under which surveillance is conducted. For example, the government may use Federal Rule of Criminal Procedure 41 without regard to FISA because Rule 41 is a criminal rule. Correspondingly, it may use FISA without regard to Title III because FISA is a foreign intelligence statute. Alternatively, *Torres* can be read to make the inquiry turn on the nature or purpose of the particular surveillance, rather than the statute under which it is conducted. In practical terms, however, the result is largely the same because the requirements of the criminal surveillance statutes effectively guarantee a law enforcement purpose. See, *e.g.*, 18 U.S.C. §§ 2516(1), 2518(1)(b), 2518(3)(a), 2518(5), 2703(a), 3122(b)(2), Fed. R. Crim. P. 41(c). (This inquiry is similar to the one required by the first clause of the exclusivity provision with respect to surveillance techniques that are not "electronic surveillance" under FISA.) Of course, where the government has a mixed purpose, it would be free to use either FISA or the criminal statutes if it could satisfy their requirements. The FISA Court of Review's decision has cleared away most of the underbrush surrounding FISA's own "purpose" requirements. See *In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

Either way, *Torres* et al. render somewhat superfluous the first part of the exclusivity provision, which provides that the law enforcement surveillance statutes do not affect the government's acquisition of "foreign intelligence information from international or foreign communications . . . utilizing a means other than electronic surveillance as defined in [FISA]." But some redundancy is understandable here, particularly because this language was adopted "to make clear that the legislation does not deal with certain international signals intelligence currently engaged in by the National Security Agency and electronic surveillance outside the United States." H.R. Rep. No. 95-1283, at 100. These activities outside the United States – which now may be part of NSA's conduct inside the United States – were (and are) conducted under the President's Constitutional authority and Executive Order 12333. Prior to FISA, as discussed in the text, they were protected by the national security disclaimer, 18 U.S.C. § 2511(3). With FISA repealing that disclaimer and affirmatively regulating foreign intelligence "electronic surveillance," however, it is understandable that NSA would have wanted an explicit safe harbor in the statute, even if redundant, to protect its foreign intelligence activities abroad that are not "electronic surveillance." Indeed, the first part of the exclusivity provision is largely redundant in any event because Title III does not apply to interceptions that take place abroad. See *United States* v. *Peterson*, 812 F.2d 486, 492 (9th Cir. 1987); *United States* v. *Cotroni*, 527 F.2d 708, 709 (2d Cir. 1975). And there are other redundant provisions of Title III on the books today. See, *e.g.*, 18 U.S.C. § 2511(2)(h)(i) (providing explicitly that Title III does not prohibit pen-trap surveillance, despite the Supreme Court's 1977 decision in *New York Tel. Co.* holding that pen-trap surveillance is not regulated by Title III). Like the government, see DOJ Whitepaper at 35 n.20, I am unable to say more on this topic. See note 16, *supra*.

[51] DOJ 12-22-05 letter at 4.

[52] *Clark* v. *Martinez*, 125 S. Ct. 716, 724 (2005); See, *e.g.*, *Spector* v. *Norwegian Cruise Lines*, 125 S. Ct. 2169, 2183 (2005).

[53] Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001). The AUMF provides:

SECTION 1. SHORT TITLE.

This joint resolution may be cited as the "Authorization for Use of Military Force".

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) IN GENERAL—That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

(b) War Powers Resolution Requirements—

(1) SPECIFIC STATUTORY AUTHORIZATION—Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution.

(2) APPLICABILITY OF OTHER REQUIREMENTS—Nothing in this resolution supercedes any requirement of the War Powers Resolution.

[54] 12-19-05 briefing transcript; DOJ 12-22-05 Letter at 2-3; DOJ Whitepaper at 2, 10-17.

[55] 542 U.S. 507 (2004). A four-Justice plurality concluded that the AUMF allows the detention, *id.* at 518, and Justice Thomas in dissent "agree[d] with the plurality" on that point, *id.* at 587.

[56] *Id.* at 518.

[57] Cf. *Mitchell* v. *Forsyth*, 472 U.S. 511, 530 (1985) ("The use of warrantless electronic surveillance to gather intelligence in cases involving threats to the Nation's security can be traced back to 1940, when President Roosevelt instructed Attorney General Robert Jackson that he was authorized to approve wiretaps of persons suspected of subversive activities"). *Forsyth* also illustrates the way in which the NSA surveillance program might be reviewed by the courts. See *id.* at 513-514 (discussing 18 U.S.C. § 3504).

[58] See *Berger* v. *United States*, 388 U.S. 41, 45-46 (1967).

[59] DOJ Whitepaper at 6-10 and 14-17.

[60] National Security Agency, 50th Anniversary Brochure (discussing the history of cryptography and signals intelligence in warfare from the American Revolution forward) (available at http://www.nsa.gov/publications/publi00012.cfm).

[61] Compare *Hamdi* (U.S. citizen first detained in Afghanistan), with *Padilla* v. *Rumsfeld*, 542 U.S. 426 (2004) (U.S. citizen first arrested in the United States). Subsequent proceedings involving Padilla are recounted in *Padilla* v. *Hanft*, No. 05-6396 (4th Cir. Dec. 21, 2005) (available at 2005 WL 3489526), application granted, No. 05A578 (U.S. Jan. 4, 2006) (available at 2006 WL 14310). As I understand DOJ's argument, it seems to apply equally, or almost equally, to purely domestic communications.

[62] Pub. L. 107-56, 115 Stat. 272 (2001). The AUMF passed both Houses of Congress on September 14, and was signed by the President on September 18, 2001. The Senate passed its first piece of post-attack terrorism legislation on September 13. See Beryl Howell, *Seven Weeks: The Making of the USA Patriot Act*, 72 Geo. Wash. L. Rev. 1145, 1151 (2004). By September 19, both the Administration and Members of Congress, including Senator Leahy, had drafted bills of more than a hundred pages each, including many amendments to FISA. *Id.* at 1152-1153 & n.41.

[63] Among the amendments to FISA made by the Patriot Act are the following: Sections 206 (allowing for roving FISA electronic surveillance), 207 (changing the duration of certain FISC authorization orders), 208 (increasing the number of FISC judges), 214 (amending FISA pen/trap provisions), 215 (amending FISA's "business records" provisions), 218 (changing the allowable "purpose" of FISA electronic surveillance and physical searches), 225 (providing immunity for providers who comply with FISA), 504 (authorizing coordination between intelligence and law enforcement officials), and 1003 (amending the definition of "electronic surveillance").

[64] The Supreme Court has interpreted statutes in light of their legislative "context," see *Cannon* v. *University of Chicago*, 441 U.S. 677 (1979); *Merrill Lynch* v. *Curran*, 456 U.S. 353 (1982), but the argument here is closer to the traditional one that multiple statutes – especially those enacted almost simultaneously – should be read together. See *Brown & Williamson*, 529 U.S. at 132-133.

[65] That is particularly the case because the Patriot Act amended the exclusivity provision, albeit with respect to a different issue than the one presented here. Section 204 of the Patriot Act amended the first clause of the exclusivity provision by adding a reference to Chapter 206 of Title 18, which authorizes criminal pen-trap surveillance. 115 Stat. at 281. Section 204 of the Patriot Act was subject to the sunset provision in Section 224 of the Patriot Act, and the government has continued to press for its renewal. See, *e.g.*, U.S. Department of Justice, *Fact Sheet: USA Patriot Act Provisions Set for Reauthorization* (Apr. 5, 2005) ("Section 204 also makes it clear that the statute's exclusivity provision applies to the interception of electronic communications as well as the interception of wire and oral communications") (available at http://www.usdoj.gov/opa/pr/2005/April/05_opa_163.htm).

Justice Souter advanced a similar argument in his dissenting opinion in *Hamdi*, relying on Section 412 of the Patriot Act, 8 U.S.C. § 1226a(a)(5), which requires the Attorney General promptly to begin removal proceedings against, or indict, an alien detained in the United States on national security grounds. 542 U.S. at 551. The argument with respect to the FISA provisions of the Patriot Act, however, is substantially more compelling, because – among other things – Hamdi was neither an alien nor captured in the United States, and therefore not subject to Section 412. The Patriot Act addressed "electronic surveillance" far more extensively and directly than it addressed the detention of enemy combatants on a foreign battlefield. See Curtis A. Bradley & Jack Goldsmith, *Congressional Authorization And The War On Terrorism*, 118 Harv. L. Rev. 2047, 2119 n.321 (2005). DOJ's whitepaper disputes this (page 24 n.10) by arguing that other statutes deal comprehensively with detention. Those statutes, however, were not part of the Patriot Act, and therefore do not illuminate Congressional intent in passing the AUMF.

[66] As noted above, the government relies on the fact that FISA's criminal penalty provision refers to surveillance authorized by "statute." I have not considered the rather technical question of whether the AUMF, a resolution passed by both Houses of Congress and signed by the President, is a "statute" as that term is used in FISA. I assume that it is based on the discussion on pages 23-24 of DOJ's whitepaper. Cf. *INS* v. *Chadha*, 462 U.S. 919 (1983).

[67] 50 U.S.C. § 1811 ("Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress"). It appears that this provision merely relieves the government of its obligation to seek FISC approval for surveillance; it does not seem to eliminate the substantive requirements in FISA (*e.g.*, the requirement that the government establish probable cause that the target of the surveillance is a foreign power or an agent of a foreign power). See H.R. Rep. No. 95-1720, at 34 ("The conferees intend that this period [15 days] will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency. The conferees also intend that all other provisions of this act not pertaining to the court order requirement shall remain in effect during this period.") It is not clear to me whether the government agrees with this point. See DOJ Whitepaper at 20.

[68] H.R. Rep. No. 95-1720, at 34.

[69] As noted in the text, I do not read the exclusivity provision to incorporate a wholesale exception for other surveillance statutes through FISA's penalty provision, and so I view the relationship between the exclusivity provision and the AUMF through the lens of implied repeal. If the government's interpretation were correct, and FISA really did create an exception for all other surveillance statutes, then its interpretation would have to hold even if the AUMF had been enacted before the exclusivity provision. To me, however, that hypothetical scenario illustrates the weakness in the government's position.

The government might argue that its interpretation need not hold if the two laws were enacted in reverse order. To be sure, in that scenario, Congress' failure to list the AUMF in the exclusivity provision would take on added significance. But that is true only if one accepts the premise that the exclusivity provision is meant to be a complete list of all statutory surveillance procedures. As explained in the text, the government rejects this premise, effectively treating the exclusivity provision as if it referred not only to the "procedures in FISA" but also to "the procedures in any other surveillance statute." Thus, on the government's theory, it should not matter which law came first.

[70] It may be that the government agrees, and welcomes resolution of the question. I say that because DOJ's letter and whitepaper noticeably begin with Article II – an approach that conflicts, both logically and rhetorically, with the

constitutional avoidance doctrine cited at the end of the letter. See DOJ 12-22-05 letter at 1-2; DOJ Whitepaper at 1-2.

[71] *Dames & Moore* v. *Regan*, 453 U.S. 654, 660 (1981) (quoting *Youngstown Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579, 634 (1952) (Jackson, J., concurring)).

[72] See *Keith*, 407 U.S. at 303 (citing 18 U.S.C. § 2511(3)); cf. *id.* at 308-309 & n.8, 321-322 & n.20.

[73] In *Keith*, the Supreme Court held that the President could not conduct warrantless electronic surveillance in domestic intelligence and security cases (*e.g.*, investigations of domestic terrorism), but left open the possibility that he could do so in foreign intelligence cases. 407 U.S. at 308-309 & n.8, 321-322 & n.20. The decision in *Keith* was more focused on the Fourth Amendment than on separation of powers – i.e., on whether the President may conduct such surveillance rather than on whether he may do so with or without congressional support. Although the Court held that Congress remained silent on the question, *id* at 303, the result probably would have been the same even if Congress had enacted a statute expressly authorizing warrantless domestic security surveillance. In evaluating warrantless foreign intelligence surveillance before the enactment of FISA, in the face of congressional silence, "virtually every court that had addressed the issue had concluded that the President had the inherent power to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment." *United States* v. *Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (citing cases). Four courts of appeals – the Third, Fourth, Fifth, and Ninth Circuits – upheld warrantless electronic surveillance conducted for a foreign intelligence purpose. See *id.* The D.C. Circuit suggested in dictum in a plurality opinion that a warrant would be required, but did not decide the issue, and no court ever held that a warrant was required. See *Zweibon* v. *Mitchell*, 516 F.2d 594, 633-651 (D.C. Cir. 1975). In *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), the court did not decide that question. It explained: "We take for granted that the President does have that authority [to conduct warrantless electronic surveillance in foreign intelligence cases] and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable." *Id.* at 742.

[74] See 50 U.S.C. §§ 1821-1829, added by Pub. L. 103-359, 108 Stat. 3443 (1994).

[75] See DOJ Whitepaper at 6-9. I do not necessarily agree with every aspect of DOJ's argument here.

[76] *Youngstown*, 343 U.S. at 870 (Jackson, J., concurring). Citing Justice Jackson, the Supreme Court in *Dames & Moore* identified a three-part framework for Presidential powers as follows (453 U.S. at 668-669 (internal quotations and citations omitted)):

> [1] When the President acts pursuant to an express or implied authorization from Congress, he exercises not only his powers but also those delegated by Congress. In such a case the executive action would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it. [2] When the President acts in the absence of congressional authorization he may enter a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. In such a case the analysis becomes more complicated, and the validity of the President's action, at least so far as separation-of-powers principles are concerned, hinges on a consideration of all the circumstances which might shed light on the vides of the Legislative Branch toward such action, including congressional inertia, indifference or quiescence. [3] Finally, when the President acts in contravention of the will of Congress, his power is at its lowest ebb, and the Court can sustain his actions only by disabling the Congress from acting upon his request.

The Court went on to observe that "it is doubtless the case that executive action in any particular action falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition." *Id.* at 669.

[77] See DOJ Whitepaper at 2, 11, 33-35.

[78] See *id.* at 10. Scholars have long debated this question. In one professor's view, at least, "the weight of modern scholarship takes the view that the Constitution lodges most foreign affairs powers, including the power to formulate foreign policy, with Congress. . . . [and that] those foreign affairs powers that the Constitution vests exclusively in the President – to serve as Commander in Chief of the armed forces and to receive foreign ambassadors – should be narrowly interpreted." Patricia L. Bellia, *Executive Power in Youngstown's Shadows*, 19 Const. Comment. 87, 114-115 (2002) (footnotes omitted). (For examples of work by those who favor congressional power, see, *e.g.*, Louis Henkin, *Foreign Affairs and the U.S. Constitution* (1996); John Hart Ely, *War and Responsibility* (1993); Harold H. Koh, *The National Security Constitution* (1990).) On the other side of the debate "are those who, in varying degrees, believe that the President has substantial authority in the conduct of foreign affairs and the protection of national security, including a power to formulate foreign policy." Bellia, *supra*, at 116. As Professor John Yoo, then a Deputy Assistant Attorney General in DOJ's Office of Legal Counsel (OLC), testified before Congress in 2002, "[u]nder Article II, Section I of the Constitution, the President is the locus of the entire 'executive Power' of the United States and thus, in the Supreme Court's words, 'the sole organ of the federal government in the field of international relations.'" John C. Yoo, *Applying the War Powers Resolution to the War on Terrorism*, 6 Green Bag 2d 175, 177 (2003) (footnotes omitted). Not all supporters of broad presidential power are members (or former members) of the Bush Administration. See, *e.g.*, H. Jefferson Powell, *The President's Authority Over Foreign Affairs: An Executive Branch Perspective*, 67 Geo. Wash. L. Rev. 527 (1999), and *The Founders and the President's Authority Over Foreign Affairs*, 40 Wm. & Mary L. Rev. 1471 (1999). Professor Powell worked in OLC in 1993-1994 and 1996.

[79] See 343 U.S. at 640-655.

[80] *Loving* v. *United States*, 517 U.S. 748, 757 (1996). As examples of such intrusions, the Court in *Loving* cited the following (*id.*):

> See *Plaut* v. *Spendthrift Farm, Inc.*, 514 U.S. 211, 225-226 (1995) (Congress may not revise judicial determinations by retroactive legislation reopening judgments); *Bowsher* v. *Synar*, 478 U.S. 714, 726 (1986) (Congress may not remove executive officers except by impeachment); *INS* v. *Chadha*, 462 U.S. 919, 954-955 (1983) (Congress may not enact laws without bicameral passage and presentment of the bill to the President); *United States* v. *Klein*, 13 Wall. 128, 147 (1872) (Congress may not deprive court of jurisdiction based on the outcome of a case or undo a Presidential pardon).

[81] *Id.* The Supreme Court has sometimes considered, but very rarely found, such impairment. It has rejected claims of impairment as follows:

> • Congress may enact a law requiring federal judges to serve on the United States Sentencing Commission. *Id.* (describing *Mistretta* v. *United States*, 488 U.S. 361 (1989)).
> • Congress may enact legislation requiring a federal agency to control a former President's official papers. *Id.* (describing *Nixon* v. *Administrator of General Services*, 433 U.S. 425 (1977)).
> • Courts may consider lawsuits against a sitting President for unofficial acts. *Jones* v. *Clinton*, 520 U.S. 681, 701-703 (1997).

[82] See DOJ Whitepaper at 29.

[83] *Swaim* v. *United States*, 165 U.S. 553, 557-558 (1897); cf. *Loving* v. *United States*, 517 U.S. 748, 773 (1996) ("we need not decide whether the President would have inherent authority as Commander in Chief to prescribe aggravating factors in capital cases" because Congress has delegated such authority to him).

[84] U.S. Const. Art. I, § 8, cl. 14. See *Loving*, 517 U.S. at 767-768.

[85] *Loving*, 517 U.S. at 767.

[86] *Id.* at 772.

[87] See *id.* at 756 (considering the question "whether it violated the principle of separation of powers for the President [rather than Congress] to prescribe the aggravating factors required [for a sentence of death] by the Eighth Amendment").

[88] U.S. Const. Art. I, § 8, cl. 12-13.

[89] For a discussion of appropriations and national security, see Peter Raven-Hansen & William C. Banks, *Pulling the Purse Strings of the Commander in Chief*, 80 Va. L. Rev. 833 (1994). Cf. *AFSA* v. *Garfinkel*, 490 U.S. 153 (1989) (per curiam) (not deciding whether an appropriations rider forbidding spending on a particular non-disclosure form improperly infringes on the President's Article II power).

[90] See, *e.g.*, *President Relents, Backs Torture Ban*, Washington Post, at 1 (Dec. 16, 2005) (available at http://www.washingtonpost.com/wp-dyn/content/article/2005/12/15/AR2005121502241_pf.html).

[91] Sections 1001-1006 of the Department of Defense, Emergency Supplemental Appropriations to Address Hurricanes in the Gulf of Mexico, and Pandemic Influenza Act, 2006, H.R. 2863 (Dec. 30, 2005) (hereinafter December 2005 Supplemental Appropriations Bill). The text of the bill (now a law) is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h2863enr.txt.pdf.

[92] The President's signing statement is available at http://www.whitehouse.gov/news/releases/2005/12/20051230-8.html (hereinafter Signing Statement on December 2005 Supplemental Appropriations Bill).

[93] Other provisions of the bill and the signing statement may more directly pertain to the NSA surveillance program. For example, Section 8007 of the bill provides that "[f]unds appropriated by this Act may not be used to initiate a [classified] special access program without prior notification 30 calendar days in session in advance to the congressional defense committees." In response to this, the President's signing statement explains:

> The Supreme Court of the United States has stated that the President's authority to classify and control access to information bearing on the national security flows from the Constitution and does not depend upon a legislative grant of authority. Although the advance notice contemplated . . . can be provided in most situations as a matter of comity, situations may arise, especially in wartime, in which the President must act promptly under his constitutional grants of executive power and authority as Commander in Chief of the Armed Forces while protecting certain extraordinarily sensitive national security information. The executive branch shall construe these sections in a manner consistent with the constitutional authority of the President.

[94] Section 1003(a) of the legislation provides that "[n]o individual in the custody or under the physical control of the United States Government, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment or punishment." Section 1003(d) defines the term "cruel, inhuman, or degrading treatment or punishment" as "the cruel, unusual, and inhumane treatment or punishment prohibited by the Fifth, Eighth, and Fourteenth Amendments to the Constitution of the United States, as defined in the United States Reservations, Declarations and Understandings to the United Nations Convention Against Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment done at New York, December 10, 1984." S. Treaty Doc No. 100-20 (1988). For a concise history of the treaty and the U.S. reservations to it, see S. Rep. No. 102-30, at 19-21.

[95] Edward S. Corwin, *The President: Office and Powers, 1787-1984*, at 200 (5th ed. 1984).

[96] Cf. S. Rep. No. 95-701, at 95-96 (additional views of Senator Malcolm Wallop) ("Consider the case of someone with knowledge of a band of nuclear terrorists, hiding in one of a thousand apartments in a huge complex. It would be both reasonable and easy to tap every telephone in the complex, discard all intercepts but the correct one, and gain the vital information. But that would involve 999 violations of this bill.").

[97] See *Kennedy* v. *Mendoza-Martinez*, 372 U.S. 144, 160 (1963).

[98] Many other issues would also be relevant, including the level of suspicion required before surveillance occurs; the purpose of the program; whether, when, and under what conditions the surveillance acquires the "content" of communications rather than the kind of "routing and addressing" information associated with pen-trap surveillance; and any number of logistical and technical issues raised by new surveillance capabilities. Cf. DOJ Whitepaper at 1, 5, 13 n.4, 40 (suggesting that the surveillance required reasonable suspicion of some connection to al Qaeda).

[99] 50 U.S.C. § 1805(f).

[100] As the Church Report explains:

> SHAMROCK is the codename for a special program in which NSA received copies of most international telegrams leaving the United States between August 1945 and May 1975. Two of the participating international telegraph companies – RCA Global and ITT World Communications – provided virtually all their international message traffic to NSA. The third, Western Union International, only provided copies of certain foreign traffic from 1945 until 1972. SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken. Although the total number of telegrams read during its course is not available, NSA estimates that in the last two or three years of SHAMROCK's existence, about 150,660 telegrams per month were reviewed by NSA analysts. Initially, NSA received copies of international telegrams in the form of microfilm or paper tapes. These were sorted manually to obtain foreign messages. When RCA Global and ITT World Communications switched to magnetic tapes in the 1960s, NSA made copies of these tapes and subjected them to an electronic sorting process. This means that the international telegrams of American citizens on the "watch lists" could be selected out and disseminated.

S. Rep. No. 94-755, Book III, at 765; see also *id.*, Book, II, at 169 (SHAMROCK "involved the use of a Watch List from 1967-1973. The watch list included groups and individuals selected by the FBI for its domestic intelligence investigations and by the CIA for its Operation CHAOS program [which involved opening international mail]. In addition, the SHAMROCK Program resulted in NSA's obtaining not only telegrams to and from certain foreign targets, but countless telegrams between Americans in the United States and American or foreign parties abroad.").

> Based on affidavits from the NSA, the D.C. Circuit has described watchlisting as follows:
>
> NSA monitors radio channels. Because of the large number of available circuits, however, the agency attempts to select for monitoring only those which can be expected to yield the highest proportion of foreign intelligence communications. When the NSA selects a particular channel for monitoring, it picks up all communications carried over that link. As a result, the agency inevitably intercepts some personal communications. After intercepting a series of communications, NSA processes them to reject materials not of foreign intelligence interest. One way in which the agency isolates materials of interest is by the use of [l]ists of words and phrases, including the names of individuals and groups .... These lists are referred to as "watch lists" by NSA and the agencies requesting intelligence information from them.

*Salisbury* v. *United States*, 690 F.2d 966, 968-969 (D.C. Cir. 1982) (citations omitted, ellipsis in original). For a more complete discussion of NSA watchlisting and FISA, see H.R. Rep. No. 98-738, at 5-6.

[101] 431 U.S. 606 (1977).

[102] *Id.* at 619.

[103] *Id.*

[104] *Id.* at 620 (citations omitted).

[105] DOJ Whitepaper at 5; see *id.* at 40.

[106] *Id.* at 1, 13 n.4.

[107] See *Alabama* v. *White*, 496 U.S. 325, 330 (1990) ("Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause").

[108] Georgetown Prepared Remarks, *supra* note 16.

[109] 338 U.S. 160, 175 (1949); see also *Illinois* v. *Gates*, 462 U.S. 213, 240-241 (1983).

[110] See cases discussed in note 73, *supra*.

[111] Cf. *Keith*, 407 U.S. at 323 (inviting Congress to authorize domestic security surveillance based on probable cause of "circumstances more appropriate to domestic security cases" but not suggesting the use of a reasonable suspicion standard).

[112] DOJ Whitepaper at 41.

[113] *Id.* at 25 n.12.

[114] Responses to Joint Questions from House Judiciary Committee Minority Members, Response to Question 32 (released March 24, 2006) (italics in original) [hereinafter HJC Minority QFRs (3-24-06)].

[115] *Id.* (second alteration in original).

[116] *Id.* at Response to Question 34.

[117] See 50 U.S.C. § 1805(a)(4) (to issue an order authorizing electronic surveillance, the court must find that "the proposed minimization procedures [in the government's application] meet the definition" of that term in the statute).

[118] 50 U.S.C. § 1805(e)(3).

[119] Hearings Before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence of the House of Representatives, on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632, the Foreign Intelligence Surveillance Act of 1977, 95th Cong., 2d Sess. at 26-31 (1978) (available at http://www.cnss.org/fisa011078.pdf). I am indebted to Marty Lederman for directing me to this source.

[120] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[121] See, *e.g.*, *Stanford* v. *Texas*, 379 U.S. 476 (1965).

[122] Cf. *Mistretta* v. *United States*, 488 U.S. 361 (1989) (United States Sentencing Commission).

[123] That could be accomplished by creating new 50 U.S.C. § 1801(f)(5) as follows: "Notwithstanding subsections (1)-(4) of this section, 'electronic surveillance' does not include the acquisition of information from an international communication."

[124] The government has stated that there are "procedures . . . in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons." HJC Minority QFRs (3-24-06), Response to Question 10.

[125] H.R. Rep. No. 95-1283, at 55.

[126] 50 U.S.C. § 1802 provides in pertinent part as follows:

> (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that –
>
> (A) the electronic surveillance is solely directed at –
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;
>
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
>
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.
>
> (2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.
>
> (3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless –
>
> (A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or
>
> (B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title.
>
> (4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to –
>
> (A) 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

(B) 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 for furnishing such aid.

[127] *Id.*

[128] See *United States* v. *Ramsey*, 431 U.S. 606 (1977).

[129] The definition is as follows: "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."

[130] HJC Minority QFRs (3-24-06), Response to Question 40.

[131] Compare 50 U.S.C. § 1801(e)(1)(A)-(B), with 50 U.S.C. § 1801(e)(1)(C) and (e)(2).

[132] See 18 U.S.C. § 3127(3) and (4); 50 U.S.C. § 1841(2).

[133] 18 U.S.C. § 2510(8).

[134] See, *e.g.*, Robert Ditzion, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 Am. Crim. L. Rev. 1321 (2004); U.S. Attorney's Manual § 9-7.500.

[135] The government has reported that under the NSA program, "[i]ntelligence officers are not making the determination of what is 'reasonable' under the Fourth Amendment; instead, they make a factual determination that the 'probable cause' standard is met in a particular instance." Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the Senate Committee on the Judiciary, Written Questions from All Democratic Senators, Response to Question 25 (released March 24, 2006) [hereinafter SJC Minority QFRs (3-24-06)].

In some ways, this would be stricter than FISA's ordinary standards, because it would require probable cause of a nexus between the agent of a foreign power and the particular communication being monitored, not merely between the agent and the telephone line carrying the communication. See 50 U.S.C. §§ 1804(a)(4)(A)-(B), 1805(a)(3)(A)-(B). But based on what I have seen in the government's public statements, using communications, rather than facilities, as the unit of analysis may make more sense here for operational reasons. Alternatively, the language in the draft could be changed to conform to that in traditional FISA – i.e., there must be probable cause that the communication is transmitted on a facility that is being used, or is about to be used, by a foreign power or an agent of a foreign power.

[136] HJC Minority QFRs (3-24-06), Response to Question 2.

[137] Letter of February 28, 2006, from Attorney General Alberto Gonzales to Senator Arlen Specter at 3 (emphasis added).

[138] 50 U.S.C. § 1801(h).

[139] See 50 U.S.C. § 1808(a)(1).

[140] See 50 U.S.C. § 1805(f).