Set forth below is a preliminary discussion of the statutory and constitutional issues raised by recent disclosures about an electronic surveillance program conducted by the National Security Agency (NSA).[1] I am not yet at rest with the analysis because the relevant facts are unavailable and the legal questions presented are complex. I have used the notes, rather than text, for the most arcane or uncertain elements of the argument.

With those caveats, the discussion can be summarized as follows: (1) NSA engaged in foreign intelligence "electronic surveillance" as defined by FISA,[2] the Foreign Intelligence Surveillance Act; (2) FISA's "exclusivity provision"[3] prohibits such surveillance except under the "procedures" in FISA; (3) the September 2001 Authorization to Use Military Force (AUMF),[4] as interpreted by the Supreme Court in *Hamdi* v. *Rumsfeld*,[5] 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.

As of this writing, the government's best legal defense of the NSA program appears in a letter from the Department of Justice (DOJ) to certain Members of Congress dated December 22, 2005, and a whitepaper released by DOJ on January 19, 2006.[6] 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.[7] 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.

* * *

1. 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."[8] He also said that FISA "requires a court order before engaging in this kind of surveillance."[9] 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."[10] The definition is even broader as applied to the targeting of United States persons – *e.g.*, a citizen or green-card holder.[11]

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."[12] It "assume[s] . . . that the activities described by the President constitute 'electronic surveillance' as defined by FISA,"[13] although it also argues that the definition produces some anomalies in light of changing technology and other factors.[14] 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.[15] Following the government's lead, I assume that NSA engaged in "electronic surveillance" as defined by FISA.

2. 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."[16] 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.[17]

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.[18]

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).'"[19]

Indeed, FISA repealed a provision of Title III disclaiming any intent to limit the "constitutional power of the President" in this area.[20] This disclaimer provision, the Supreme

Court held in 1972, "simply left presidential powers where it found them."[21] 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."[22] 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."[23] 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.[24]

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."[25] 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."[26] 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.[27] 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,[28] courts likely would overcome their normal aversion, and find an implied repeal (or amendment) of the latter by the former.[29] An ambiguous new statute, however, would be read not to authorize electronic surveillance in order to avoid a conflict with the exclusivity provision.[30] 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."[31] 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]."[32] 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.'"[33]

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.[34] 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."[35] 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.[36] 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."[37] 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.[38] 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."[39] 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."[40]

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.[41] 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.[42]

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.[43] 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."[44] 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"[45] – as well as the statute's rules permitting electronic surveillance in certain circumstances without the FISC's approval.[46] 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.[47]

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."[48] 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."[49] 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.

3. 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),[50] a joint resolution passed by Congress and signed by the President shortly after the September 11, 2001, attacks.[51] In *Hamdi* v. *Rumsfeld*, the Supreme Court concluded that the AUMF authorized the use of military detention.[52] 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."[53]

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;[54] electronic surveillance of telegraph signals was apparently conducted as early as the Civil War.[55] DOJ's whitepaper traces this history in detail,[56] and the NSA has published an informative study on the history of signals intelligence in war that makes similar assertions.[57] 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.[58]

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.[59] The Patriot Act, of course, substantially amended FISA to aid the government's efforts against terrorism.[60] 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."[61] 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.[62]

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.[63]

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.[64] 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."[65] 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.[66] 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.

4. 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?[67] 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."[68] 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.

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

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."[73] The government accepts this.[74] 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?[75] 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).[76] 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."[77] As a functional matter, the question is whether one branch has unduly "impair[ed] another in the performance of its constitutional duties."[78] DOJ appears to agree that these are the relevant tests.[79]

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.[80] 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."[81] The Court has said that under this clause Congress "exercises a power of precedence over . . . Executive authority."[82] But could Congress forbid the President from <u>ever</u> 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."[83] 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.[84]

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."[85] 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.[86] 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,[87] Congress in December 2005 passed, and the President signed, a law that would ban the torture of such detainees.[88] 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."[89] 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.[90] In such instances, the President apparently believes, his power to torture is plenary.[91]

All of these real and hypothetical examples illustrate what Professor Corwin famously called the Constitution's "invitation to struggle" for dominance in foreign affairs.[92] 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.[93] The Constitution is not a suicide pact.[94]

The second question concerns the reasons for eschewing the use of FISA in obtaining the information.[95] For example, if FISA did not contain an emergency exception,[96] 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).

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 far more hostility. A reprise of something like Operation Shamrock,[97] for example, supported by arguments that FISA simply requires too much paperwork, would be very problematic. A lot turns on the facts.[98]

-- David Kris, January 25, 2006.[99]

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

[3] 18 U.S.C. § 2511(2)(f).

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

[5] 542 U.S. 507 (2004).

[6] 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).

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

[8] 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").

[9] 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 46, *infra*.

[10] 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.

[11] 50 U.S.C. § 1801(f)(1). The term "United States person" is defined in 50 U.S.C. § 1801(i).

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

[13] *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). As discussed in note 10, *supra*, the term "electronic surveillance" does not include, and FISA therefore does not regulate, (1) surveillance that occurs abroad of a target that is located abroad; and (2) surveillance in which all parties to the acquired communication are located abroad, regardless of where the surveillance occurs. See H.R. Rep. No. 95-1283, at 50 n.24.

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

[15] 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). Compare discussion in note 13 , *supra*.

[16] 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 27, *infra*.

[17] *Id.*

[18] 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).

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

[20] 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."

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

[22] 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 47, *infra*.

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

[24] 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.

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

[26] 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).

[27] 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 16, *supra*. The Patriot Act's amendment to the exclusivity provision is discussed further in note 62, *infra*.

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

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

[30] 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).

[31] DOJ Whitepaper at 20.

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

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

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

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

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

[37] 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.

[38] *Id.*

[39] 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;