Written Testimony of David S. Kris before the
Senate Select Committee on Intelligence,
May 24, 2005

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee: Thank you for the opportunity to testify about the Foreign Intelligence Surveillance Act (FISA) and related provisions in the Committee's draft bill. I join the Department of Justice (DOJ) in applauding the bill for addressing several difficult and important issues. Having first seen it less than a week ago, however, I have not yet mastered all of its policy implications or technical aspects. This is a very complicated area of law. Accordingly, while I pledge my continuing availability, this morning I can offer only tentative views based on a few days' consideration. Subject to that caveat, set forth below are a few general comments, and several specific comments, on the bill. In appearing before you today, I speak only for myself, and not for any former or current employer, including DOJ and Time Warner.

In general, the Committee's draft bill authorizes and regulates several vitally important investigative tools, and I am therefore not surprised that DOJ has expressed its support. For example, Sections 101 and 203 will prevent any resurgence of the FISA "wall" separating intelligence and law enforcement. As I testified in the House last month,[1] the wall is extremely dangerous; this bill will help keep it down. Section 101 of the bill will also help ensure the government's continuing authority to conduct "roving" FISA surveillance, a tool that appears to be very valuable, and that already contains strong protections for civil liberties. Section 102 makes permanent the lone-wolf provision of FISA, which I understand DOJ strongly supports. Two other provisions of the bill, Sections 201 and 216, will likely ease administrative burdens on the FBI and DOJ by extending the duration of FISA authorization orders involving non-U.S. persons (Sections 214 and 215 may have similarly helpful effects). In an era of increasing FISA activity, this helps focus resources on cases involving U.S. persons, where civil liberties concerns are preeminent.

This bill should also enjoy substantial support from civil libertarians. For example, Section 213 would authorize administrative subpoenas that are similar to existing national security letters, but with an express provision for motions to quash. Another part of the bill, Section 211, would expand the disclosure rights of persons who receive a FISA tangible things order, and permit them to consult with counsel. Section 211 would also require special minimization procedures governing the retention and dissemination of information obtained from a tangible things order. And it would expand the government's reporting obligations.

I do have questions about certain provisions in the bill. In Sections 202 and 212, for example, I wonder whether it offers legislative solutions to problems that the Executive Branch ought to be able to resolve internally. I believe that Congress should change FISA only to address specific shortcomings not amenable to other remedies. However, I also think that law and policy should reflect operational experience. My own operational experience in this area, once extensive, is now two years out of date. I may not recognize or understand all of the problems facing government today. The Department of Justice, and you and your staff, are the

real experts in this area, and I hasten to defer to your expertise. In any event, I do not think that Sections 202 and 212 threaten civil liberties.

Finally, in evaluating this bill, particularly Section 213, I urge you to consider not only whether "the government" – meaning the Executive Branch as a whole – should have certain investigative power, but also which parts of government should have power. Although I have no doubts about the constitutionality or importance of Section 213, I believe strongly that government is more effective, and civil liberties are better protected, when FBI agents and DOJ lawyers work as closely and cooperatively in national security investigations as they do in traditional criminal investigations. Until late 2002, of course, the FISA wall effectively prohibited this. As we emerge from the shadow of the wall, broad structural changes, such as the creation of a DOJ National Security Division, may be necessary to foster the cooperative model. But substantive bills like the Committee's draft should also do so where they can.

Thank you again for the opportunity to be here. The balance of this submission presents a section-by-section review of the Committee's draft bill. Again, in light of the complexity of the legal issues and the speed with which I have prepared this testimony, I emphasize the tentative nature of my comments.

SECTIONS 101, 102 and 203

Sections 101 and 102 of the Committee's draft bill are designed to eliminate the upcoming sunset for several provisions of the USA Patriot Act,[2] and for the lone-wolf provision of last year's Intelligence Reform and Terrorism Prevention Act.[3] You and your counterparts in the House of Representatives have already heard from many witnesses on both sides of the sunset debate. By and large, I support renewal of the Patriot Act, but I would like to focus today on two important provisions: Section 218 of the Patriot Act, the "significant purpose" amendment to FISA (in connection with which I also discuss Section 203 of the Committee's bill); and Section 206 of the Patriot Act, the "roving surveillance" amendment to FISA.

1. Patriot Act Section 218: Significant Purpose.

On April 28, 2005, I testified about Section 218 before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee.[4] My position then (as now) was that Congress should renew Section 218. I also urged the Subcommittee explicitly to endorse the reasoning and decision of the Foreign Intelligence Surveillance Court of Review (FISCR or Court of Review) interpreting Section 218 and other provisions of FISA.[5] I testified:

> Whether or not you agree with its outcome, the Court of Review's opinion is a very sophisticated and technically sound interpretation of a complex statute. If Congress were to adopt its reasoning, it would provide guidance that is equally sophisticated and sound. That, above all, is what the country needs in this area.[6]

I maintain that view today, and I therefore renew my recommendation that Congress adopt the Court of Review's reasoning, either through explicit legislative history or a specific provision of public law.[7]

Repealing the sunset for Patriot Act Section 218 intersects with another provision of the Committee's bill, Section 203. Section 203 would amend the definition of "foreign intelligence information" to make explicit that information is "foreign intelligence information" even if it is sought for use in law enforcement efforts (such as criminal prosecution) to protect against terrorism and other foreign intelligence threats.[8] As a technical matter, I believe that Section 203 will accomplish what it is evidently meant to accomplish – that is, it will make clear Congress's intent to allow FISA searches or surveillance for the primary purpose, or even the exclusive purpose, of obtaining evidence for the prosecution of a foreign spy or terrorist.[9]

As a policy matter, however, you know from my House testimony that I do not support such an amendment for two reasons.[10] First, Section 203 of the Committee's bill would further expand governmental power at a time when the Department of Justice itself has not asked for broader authority. Second, a related point, I fear that any operational benefit from the amendment would not justify the resulting cost in uncertainty about the state of the law. As I

stated at the outset, I believe that FISA should not be amended except where the amendment is genuinely necessary.[11]

If you disagree, and decide to enact Section 203 of your bill, you should consider how it will interact with Patriot Act Section 218. That is because, when read together, the two provisions could produce strange results. As explained above, Section 203 would allow the government to use FISA exclusively, not just primarily, to gather evidence for the prosecution of a foreign spy or terrorist – because Section 203 defines "foreign intelligence information" to include evidence sought for such a prosecution. Under Patriot Act Section 218, however, acquisition of "foreign intelligence information" need only be a "significant purpose" of a FISA search or surveillance. Thus, with both provisions on the books, the government might have authority to use FISA for a significant purpose of prosecuting a spy or terrorist, but the primary purpose of something else – ranging from ordinary law enforcement, to civil debt collection, to (maybe) sheer voyeurism.[12] I myself support the status quo through renewal of Patriot Act Section 218 and adoption of the Court of Review's decision. A reasonable person might disagree and prefer Section 203 of your bill. If you both renew Section 218 and enact Section 203, I recommend that you include strong legislative history to guard against any misreading.

2. Patriot Act Section 206: Roving Surveillance.

I believe the current debate over roving FISA surveillance has gone awry. Some have claimed that under Patriot Act Section 206, "[t]he government can now issue 'John Doe' roving wiretaps that fail to specify a target or a telephone, and can use wiretaps without checking that the conversations they are intercepting actually involve a target of the investigation."[13] I disagree. As I try to demonstrate below by analyzing the two statutes, FISA's rules on roving surveillance compare favorably with those in Title III,[14] its counterpart in conventional criminal law.

a. Title III.

The conduct that fundamentally justifies and underlies all Title III electronic surveillance is the commission of a specified criminal offense.[15] To obtain a normal (non-roving) surveillance order under Title III, the government must identify the offense.[16] However, it need not identify or describe the person suspected of committing the offense,[17] and it need not establish a nexus between any person and the location, telephone, or other facility to be monitored. Instead, under Title III, the government establishes a nexus between the offense and the location, telephone or other facility to be monitored.[18]

By contrast, when the government obtains a roving surveillance order under Title III, these requirements are effectively reversed. For obvious reasons, in such cases, the government must identify the person committing the specified offense and whose communications are to be intercepted.[19] However, the government need not identify the facilities from which or the place where the communications are to be intercepted, and it need not establish a nexus between those

facilities or places and the specified offense.[20] Unlike ordinary Title III surveillance, roving Title III surveillance focuses on the target, not the facility being used in connection with a crime.[21]

To use Title III's roving surveillance provisions, the government must also make certain additional showings. To obtain a roving surveillance order with respect to what Title III defines as "oral communications,"[22] the government must persuade the court that it is not "practical" to establish a nexus between the underlying conduct and the location to be monitored,[23] and may not begin the monitoring until "the place where the communication is to be intercepted is ascertained."[24] With respect to what Title III defines as "wire communications"[25] or "electronic communications"[26] the government must establish probable cause that the actions of the person committing the underlying conduct "could have the effect of thwarting interception from a specified facility,"[27] and the roving surveillance order must be "limited to interception only for such time as it is reasonable to presume that the person * * * is or was reasonably proximate to the instrument through which such communication will be or was transmitted."[28]

b. FISA.

FISA establishes a different regime. In a normal (non-roving) FISA case, the government must identify or describe the target of the surveillance,[29] and must also show that the target is engaged in the underlying conduct that justifies the surveillance.[30] Under FISA, of course, that underlying conduct is whatever makes the target a foreign power or an agent of a foreign power, which may (but need not always be) criminal conduct – *e.g.*, for a U.S. person, knowing engagement in international terrorism, or for a non-U.S. person, serving as a foreign country's diplomat in the United States.[31] The government must also establish a nexus between the target and the facility to be monitored, by showing that the target is using, or about to use, the facility.[32] However, the government need not establish a nexus between the target's underlying conduct and the facility – *e.g.*, it need not show that the facility is being used in connection with international terrorism.[33]

All of the foregoing requirements apply equally to roving FISA surveillance. The only difference between ordinary and roving FISA surveillance is that in a roving case, where the FISC "finds that the actions of the target * * * may have the effect of thwarting the identification of a specified person" who can assist the government in accomplishing the electronic surveillance, the FISC may order such assistance from "other persons" as well as the specified persons normally included in a secondary order.[34] Thus, for example, rather than issuing a secondary order directing assistance from a particular telecommunications company, the FISC can issue a generic order directing any telecommunications company to assist the government. The government can use this order to follow the target wherever he goes.

Or can it? As discussed above, in normal surveillance cases, both Title III and FISA require some showing of a nexus between the telephone or other facility that will be wiretapped, and either the target (under FISA)[35] or the specified criminal offense (under Title III).[36] Title III eliminates that nexus requirement in roving cases – on the theory that in such cases the

government cannot make the showing because it "may not know, until shortly before the communication, which telephone line will be used by the person under surveillance."[37] FISA seems to recognize this same theory, because (as amended in 2002) it requires the FISC's authorization order to specify the nature and location of each facility to be surveilled only "if known."[38] Nonetheless, FISA does not eliminate the nexus requirement: In roving cases as well as ordinary cases, it demands probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[39] How can the government make that showing in a roving case, where – by definition – it cannot even identify the facilities or places at the time the FISC enters its order?

In my view, the best answer lies in FISA's minimization provisions. As you know, those provisions require the Attorney General to propose, and the FISC to approve (as proposed or as modified), specific procedures "that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition * * * of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain * * * foreign intelligence information."[40] If the minimization procedures require a nexus before the government commences roving surveillance on a new facility – *e.g.*, through observation of the target using the facility, or some other method – they ought to satisfy the requirement that each facility "is" being used or about to be used by the target before the surveillance begins.[41]

In practical effect, instead of finding probable cause with respect to particular facilities not yet known, the FISC finds that there necessarily will be probable cause under the minimization procedures it imposes as part of its authorization order. This is roughly equivalent to Title III's provisions eschewing a formal nexus requirement to any particular facility but requiring that roving surveillance of wire or electronic communications be "limited to interception only for such time as it is reasonable to presume that the [target] * * * is or was reasonably proximate to the instrument through which such communication will be or was transmitted."[42] It is broader than Title III in that it could be satisfied by something other than proximity to a communications instrument (*e.g.*, where the target uses one facility to communicate through another, remote facility), but it is narrower in that mere proximity is not necessarily sufficient (*e.g.*, where the target walks past a pay phone but does not use it).

c. Conclusion.

In light of the foregoing, if I am reading the statute correctly, it is ironic that civil libertarians have raised concerns about "John Doe" roving FISA orders. Every provision in FISA that applies to ordinary surveillance applies to roving surveillance; there are no exceptions. One of those FISA provisions requires probable cause that the target is using, or is about to use, "each" facility subjected to surveillance. As a question of roving surveillance compared to ordinary surveillance, you literally could not ask for more (other than, perhaps, what I describe in the next paragraph).[43]

There is one amendment to FISA that might address some of the concerns raised by civil libertarians without unduly inhibiting the government. In essence, FISA roving surveillance resembles a highly circumscribed form of emergency surveillance. In a typical emergency surveillance case, the government determines unilaterally whether it can satisfy all of the provisions of FISA (subject to later ratification by the FISC).[44] In a roving case, the government determines unilaterally only whether it can satisfy the nexus requirement (the FISC determines in advance all other issues, such as whether the target is an agent of a foreign power). As in emergency cases, therefore, it may be worth considering whether the government should be required to submit to the FISC, within some reasonable time after commencing roving surveillance on a new facility, a description of the information upon which it relied to do so. Such a provision would read something like this:

> SEC. XXX. REPORT IN ROVING SURVEILLANCE CASES.
>
> Subsection 105(c)(2) of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1805(c)(2)) is amended by adding the following new subsection (E):
>
> > that, in any case in which the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person as described in subsection (c)(2)(B) of this section, and in which the electronic surveillance is directed against any facility or place the nature and location of which is not specified in the Court's order under subsection (c)(1)(B) of this section, the applicant or another Federal officer promptly report to the Court the information relied upon determine that the target of the surveillance was using, or was about to use, such facility or place.

This amendment should assuage fears about FISA roving surveillance by requiring judicial review, albeit shortly after the fact. Obviously, if the FISC found the government's submission unsatisfactory, it could terminate surveillance on the new facility (on the theory that the government had not complied with the minimization procedures).

I do not know what the Department of Justice will say in response to this amendment, but it seems reasonable to me in concept. If the word "promptly" is unsatisfactory for any reason – I borrowed it from 50 U.S.C. § 1824(c)(2)(E), the provision requiring the government to file a return following execution of a physical search – a fixed period (3 days, 7 days, 10 days), or a "reasonable period to be determined by the Court," could be used instead.

SECTIONS 201 & 216

Section 201 of the Committee's bill would amend FISA's definition of "agent of a foreign power" in 50 U.S.C. § 1801(b)(1)(A). As you know, 50 U.S.C. § 1801(b)(1)(A) currently applies to any non-U.S. person who "acts in the United States as * * * a member of" a group engaged in international terrorism or activities in preparation therefor.[45] Another provision, 50 U.S.C. § 1801(b)(2)(E), currently applies to any person (including a U.S. person) who "knowingly aids or abets any person in the conduct of," or "knowingly conspires with any person to engage in," sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power.[46] Section 201 of the bill would add to 50 U.S.C. § 1801(b)(1)(A) the aiding-and-abetting and conspiracy language from 50 U.S.C. § 1801(b)(2)(E).

This proposal would not change FISA's definitions in any substantive way. It would neither expand nor contract the reach of FISA, because anyone who would fall under Section 201 of the bill is already covered by 50 U.S.C. § 1801(b)(2)(E). The principal effect of Section 201 would be to extend the duration of FISA search or surveillance orders applicable to such persons (if they are not U.S. persons), from 90 days, to an initial order of 120 days and renewal orders of 1 year each.[47] A subsidiary effect would be to eliminate FISA's civil damages remedy for such persons.[48]

As a policy matter, Section 201 seems reasonable. If longer periods of surveillance and search authority are appropriate for non-U.S. persons who are "members" of groups engaged in international terrorism or activities in preparation therefor,[49] then they seem tolerable for non-U.S. persons who knowingly aid and abet or conspire to engage in sabotage, international terrorism, or activities in preparation therefor. In keeping with my basic view that FISA should be amended only when necessary, however, I would defer to the Department of Justice on whether Section 201 of the bill would in fact ease a burden – by reducing the number of applications that must be filed – or otherwise solve a real problem in the administration of the statute.

Section 216 is a related provision that specifically amends the duration provisions of FISA. Under Section 216, FISA electronic surveillance and physical searches targeting non-U.S. persons who are agents of foreign powers could be conducted for an initial period of 120 days and for renewal periods of one year. This would change current law, under which those longer authorization periods apply only to officers or employees of foreign powers, and to members of international terrorist groups.[50] If Section 216 is enacted, Section 201 becomes superfluous (except for its effect on FISA's civil damages remedy as discussed above). (Of course, there is nothing wrong with including both provisions in the bill at this stage of the legislative process.) Section 216 would also extend from 90 days to one year the initial and renewal authorization periods for FISA pen-trap surveillance where the applicant certifies that the "information likely to be obtained is foreign intelligence information not concerning a United States person."

SECTION 202

Section 202 of the bill would amend FISA's definition of "contents"[51] essentially to conform to the definition of the same term in Title III.[52] I think I understand the motivation for this amendment, but I question the need for it.

Since its enactment in 1978, FISA has allowed the government to seek, and the FISC to issue, orders authorizing pen-trap surveillance. For the first 20 years of the statute's existence, however, the government could do so under FISA only by satisfying the requirements for a full-content "electronic surveillance" order.[53] In 1998, Congress amended FISA to allow the government to obtain pen-trap orders under a different, and less demanding, set of standards.[54]

FISA's 1998 provisions define the terms "pen register" and "trap and trace device" by reference to the pen-trap provisions applicable in criminal investigations.[55] Under the criminal provisions, a pen register is

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.[56]

Reduced to its essentials, this definition means that a pen register is supposed to detect the destination of outbound communications from a monitored telephone or other facility, without detecting the contents of the communication being sent.[57] A pen register on your telephone can identify whose number you call, but not what you say if someone answers.

A trap and trace device is the reciprocal of a pen register: It is supposed to detect the source of inbound communications to a monitored facility. Thus, a trap and trace on your telephone can identify whose telephone number called you, but not what you say. As a technical matter, a trap and trace device defined to be

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.[58]

Since 2001, a pen register and a trap and trace device may either be a "device" or a "process," which includes software as well as hardware methods of gathering information.[59]

Typically, pen register orders are used to obtain the numbers being dialed from a targeted telephone number, and trap and trace orders obtain the numbers of telephones making calls to a targeted number.[60] Under amendments enacted in the Patriot Act, however, neither FISA nor the criminal pen-trap statute is limited to telephone numbers. Those statutes may now be used to obtain any "dialing, routing, addressing, or signaling information" that identifies the destination or source of an electronic communication, including email and Internet communications.[61] But a pen-trap order may not be used to obtain the "contents of any communication."[62]

Although FISA itself defines the term "contents," that definition does not govern FISA pen-trap surveillance.[63] Indeed, if it did apply, the statute would effectively forbid what it authorizes, because FISA defines "contents" to include "any information concerning the identity of the parties to [a] communication or the existence * * * of that communication"[64] – a standard that clearly includes the routing and addressing information acquired by a pen-trap.

This, I believe, is the concern that underlies Section 202 of the Committee's bill: A concern that FISA's broad definition of "contents" somehow calls into question the validity of FISA pen-trap surveillance.[65] I believe the concern is misplaced for two reasons.[66]

First, FISA's pen-trap provisions clearly take their definition of "contents" from Title III,[67] which (as noted above) defines the term more narrowly than FISA to mean "any information concerning the substance, purport, or meaning of [a] communication,"[68] but does not include information concerning the identity of the parties or the existence of the communication. Thus, a FISA pen-trap order allows acquisition of routing and addressing information that is not "contents" as defined by Title III, even if such information is "contents" as defined by FISA. Put another way, having narrowed Title III's definition of "contents" in 1986,[69] and cross-referenced the narrower definition in FISA's pen-trap provisions, you need not amend FISA's definition of "contents" today.

Second, FISA's pen-trap provisions, and their incorporation of Title III's narrow definition of "contents," do not conflict with FISA's electronic surveillance provisions and their broad definition of "contents." On the contrary, FISA authorizes pen-trap surveillance "[n]otwithstanding any other provision of law" and "in addition to the authority" granted to conduct electronic surveillance.[70] Thus, FISA pen-trap surveillance remains lawful, and there is no need for any change to FISA's definition of "contents."

In sum, FISA seems clearly to authorize pen-trap surveillance without a full-blown "electronic surveillance" order issued under 50 U.S.C. § 1805. The government has in fact been conducting FISA pen-trap surveillance for many years. If agents or others in the Executive Branch remain concerned, perhaps it highlights the need for more training and outreach efforts. But I am not aware of any statutory problem in need of repair.

SECTION 211

Section 211 amends FISA's "tangible things" provisions in four ways. First, it makes two changes to the language of 50 U.S.C. § 1861(a)(1). As amended by Section 211, 50 U.S.C. § 1861(a)(1) would provide (with deleted text in ~~strikeout~~ and added text in redline):

> The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) ~~for~~ relevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities~~, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution~~.

I have no objection to the first change – replacing "for" with "relevant to."[71] And in view of the First Amendment provision that remains in 50 U.S.C. § 1861(2)(B),[72] I have no objection to the Committee's deletion of what amounts to a redundant First Amendment provision from Section 1861(a)(1).

Second, Section 211 would change the non-disclosure provision in the tangible things statute. Today, that provision states simply that "[n]o person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section."[73] Section 211 would add several exceptions to this general prohibition, including disclosure to "an attorney to obtain legal advice with respect to the production of things in response to the order," and "other persons as permitted by" the FBI Director or his designee. Recipients of disclosure are subject to the same general non-disclosure obligations and must be so advised by the person making the disclosure to them.

These changes seem to be motivated by (and reasonable in light of) *Doe* v. *Ashcroft*,[74] which struck down on First Amendment grounds a similar non-disclosure provision in one of the national security letter statutes.[75] The court in *Doe* recognized that "the Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one," and that non-disclosure rules further that interest.[76] But the court found that the "categorical, perpetual, and automatic ban on disclosure is not a narrowly-tailored means to advance those legitimate public interests."[77]

I don't know whether *Doe* was correctly decided – I believe the government has appealed – but it seems reasonable in any event to consider additional exceptions to the non-disclosure rules in FISA's tangible things provisions. Of course, any exception creates some risk – disclosure to a lawyer could be dangerous, as illustrated by the recent prosecution of Lynne

Stewart – but there is no way to keep the orders absolutely secret. More importantly, I am very sympathetic to persons who receive these strange-looking papers from the FISA Court by way of the FBI. I know the FISA statute pretty well, but if someone handed me a tangible things order, I'd want to consult with a lawyer before responding.[78]

An additional disclosure exception, not presently in Section 211 of the Committee's bill, may be worth considering. One of the concerns in *Doe* was the unlimited duration of the ban on disclosure. That may seem a marginal concern, but under the First Amendment, concerns at the margin of a statute's application can have far-reaching consequences.[79] I think the problem is solved, however, if the ban on disclosure endures only so long as the underlying application and order remain properly classified under the ordinary rules governing classification.[80] There should be no First Amendment problem with requiring recipients of properly classified information generally to keep it secret.[81]

Third, Section 211 would direct the Attorney General to adopt "minimization procedures governing the [FBI's] retention and dissemination" of tangible things. As a policy matter, this requirement is unobjectionable – indeed, I support the use of minimization procedures as important safeguards for civil liberties. I do, however, have a few, minor technical concerns. First, as far as I can tell, the "minimization procedures" mentioned here would not be reviewed and approved by the FISC. Thus, they are not "minimization procedures" as that term is used elsewhere in FISA.[82] If that is correct, the provision may not be necessary, at least as far as U.S. persons are concerned. Under Executive Order 12333, "[a]gencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency involved and approved by the Attorney General."[83] If the provision is to remain in the statute, and these "minimization procedures" are not meant to be reviewed by the FISC, a different term should be used to avoid confusion.

Fourth and finally, Section 211 would expand the government's reporting obligations to include the total number of tangible things orders granted, and the total number of them directed at libraries and certain other specified establishments. This seems reasonable enough, and I defer to the Department of Justice, which has recently revealed similar statistics in public testimony.[84]

SECTION 212

Section 212 amends FISA to direct the United States Postal Service to comply with a request for a mail cover from a designated official of the FBI. As far as I can tell, Section 212 codifies many of the provisions now set out at 39 C.F.R. § 233.3, and changes certain of them.[85] Normally, I would say that Section 212 presents a legislative solution to a sub-legislative problem, and that concerns about the mail cover regulations should be taken up by the FBI with the Postal Service. However, if – as I understand may be the case – sub-legislative remedies have been exhausted,[86] a statutory fix becomes more plausible. From a civil liberties perspective,

Section 212 also has the advantage of requiring Congressional oversight of the use of national security mail covers.

Under the current postal regulations, the FBI can get a mail cover by asking the Postal Service. A mail cover is available to "[p]rotect national security," a term that is defined to include most of the threats specified in the first half of FISA's definition of "foreign intelligence information."[87] To obtain a mail cover, a "law enforcement agency," which is defined to include "any authority of the Federal Government * * * one of whose functions is to * * * protect the national security,"[88] submits a written request (or when time is of the essence, an oral request[89]) to the Chief Postal Inspector or his designee with "reasonable grounds to demonstrate the mail cover is necessary to * * * Protect the national security."[90] In national security cases, a mail cover can remain in effect for 120 days, and longer with the approval of certain Postal Service officials.[91] A national security mail cover must be approved personally by the head of the agency requesting it, or by a single designee at the requesting agency's headquarters.[92]

I can understand why the FBI might chafe at certain of these requirements – particularly the one concerning high-level approval of any national security request, and the fact that compliance with a request is not mandatory. In my view, this sort of inter-agency dispute is usually best resolved within the Executive Branch.[93] Were it not for the fact that the Attorney General had personally raised this issue with the Postmaster General more than six months ago, I would be very skeptical of Section 212. As it is, I can understand DOJ's desire to seek the Committee's aid. I note with interest the Department's views letter of May 18, 2005, in which it expresses support for Section 212, and I assume (in accord with OMB Circular A-19) that the Administration does not object to that expression of support. Perhaps the possibility of a legislative amendment will concentrate the Postal Service's mind and cause it to reconsider.

SECTION 213

Section 213 of the Committee's bill would allow certain designated FBI officials to issue administrative subpoenas in the context of national security investigations authorized under Executive Order 12333[94] and not premised solely on First Amendment activities. It allows enforcement of such a subpoena by the Attorney General through the FISC, and also provides for motions to quash filed in the FISC or in the recipient's local United States District Court. Proceedings in courts other than the FISC are to be closed and subject to nondisclosure rules, and the government may submit materials to such courts *ex parte* and *in camera*. The Director of the FBI is directed to establish regulations for the implementation of the subpoena provisions, and the Attorney General is directed to establish minimization procedures governing retention and dissemination of information obtained by subpoena. There is a provision for congressional oversight through the Intelligence Committees.

The government needs the power to compel production of documents and other materials in national security investigations, and administrative subpoenas are one important way to grant such power. From a civil liberties standpoint, Section 213 is, if anything, an improvement over

current law. Unlike the current version of FISA's tangible things provisions,[95] Section 213 provides expressly for disclosure to an attorney. Moreover, unlike even the version of the tangible things provisions proposed by Section 211 of the Committee's bill, Section 213 provides for judicial review of a subpoena upon a motion to quash filed by the recipient. It allows private litigants access to the FISC, which may be viewed by civil libertarians as a good thing regardless of what is litigated. There are now several administrative subpoena provisions on the books for use in investigations pertaining to such things as health care fraud, child sexual abuse, and threats against protected persons,[96] as well as drug cases.[97] Thousands of administrative subpoenas have been issued in these kinds of cases.[98] Administrative subpoenas in national security cases, with the same or similar protections – including authorization for motions to quash – seem unobjectionable by comparison.

I have two other observations about Section 213. First, I am concerned about the invitation to private litigants to file motions in the FISC. This is not so much a philosophical concern as a pragmatic one. If thousands of subpoenas are issued, several motions to quash may be filed.[99] As far as I know, the FISC is simply not equipped to handle that kind of litigation. Indeed, the FISC is not really equipped to handle any litigation involving private parties – it has no publicly accessible space, and a relatively small staff. To be sure, these logistical obstacles could be overcome, but only by changing the FISC's nature and focus. With the dramatic increases in FISA activity over the past few years, I think the FISC should remain centered on its core function of reviewing applications. If the recent statistics revealing substantial numbers of denials and modifications of FISA applications are any guide, the FISC has been doing a careful job. I would not lightly open the FISC to adversary proceedings, particularly over something like an administrative subpoena. But I have no similar objection to motions to quash filed in ordinary district courts, as long as the government is prepared to assume the risk of a leak. And ultimately, I largely defer to the Department of Justice with respect to what is workable here, at least in the first instance.

My second concern arises because Section 213 grants administrative subpoena power to the Director of the FBI, and orders the Director to establish regulations for the use of such subpoenas. I think the authority should be granted to the Attorney General, who may delegate (and in some other cases has delegated[100]) the authority to the Director. This may seem a trivial point – and in many respects it is – but I believe it relates to a broader and vitally important concern. I think it may be helpful to the Committee if I lay out that broader concern, using Section 213 as an illustration.

As the Committee is aware, the Executive Branch is now considering whether and how to restructure the government to deal with domestic counterintelligence matters. Spurred by the 9-11 Commission Report, and the more recent WMD Commission Report, some have suggested splitting the FBI to create an American version of MI-5 – that is, a domestic counterintelligence agency separate from federal law enforcement. The FBI obviously opposes that idea. I also oppose creating an American MI-5, primarily because I think such a major change would take

years to bear fruit, and would create chaos in the interim. Unfortunately, our adversaries will not let us call a time-out while we restructure.

In my view, the more promising approach is to mandate significantly increased coordination between the FBI and DOJ prosecutors and other lawyers. Such coordination should, in my view, be required in individual cases and investigations, in national-level programs, and also in policy-making (both intra- and inter-agency). As I explained last month in my testimony before the House,[101] bringing agents and lawyers together would make the Department and the FBI more efficient and effective, and would also enhance protection of civil liberties. It would do this by taking advantage of the DOJ/FBI culture and training that have been in effect for many years in all investigative areas except national security. Agents and lawyers working together produce better results than either group working alone.

In keeping with this view, I support legislative measures that tend to unite agents and lawyers in national security investigations. Section 213 will not do that because, like the current national security letter statutes, it allows the FBI to take investigative action unilaterally. It thus stands in contrast to grand jury subpoenas, which cannot be issued without the involvement of prosecutors. I believe Section 213 should encourage cooperation between agents and lawyers by requiring lawyers' involvement, or at least by giving the Attorney General the option to do so. The Attorney General controls both DOJ proper and the FBI, and he may therefore decide to delegate administrative subpoena power directly to the FBI. On the other hand, particularly if DOJ creates a National Security Division, he might delegate the power to the head of that division, and/or to specially designated Assistant U.S. Attorneys in the field. I recommend that Section 213 be changed to grant administrative subpoena authority to the Attorney General.

SECTION 214.

Section 214 would eliminate the current requirement that the Department of Justice report to Congress on the number of cases in which FISA information has been authorized for use in criminal cases.[102] The obligation to report authorizations for use of FISA information at trial would remain.[103] If, as I hope, this provision reflects a vastly expanded administrative burden arising from vastly expanded sharing of intelligence information with law enforcement officials, then I take it as a very promising sign that dots are being connected.

SECTION 215

Section 215 would allow the government to obtain subscriber information, of the sort normally acquired by a FISA tangible things order, as part of FISA pen-trap surveillance. Thus, for example, instead of obtaining only the telephone numbers called by a monitored telephone, the government could get the telephone numbers and the names, addresses, length of service, and other information about the subscribers to those telephone numbers. This appears to be patterned after 18 U.S.C.§ 2703(c)(2). This seems like a reasonable effort to spare the government the need to file two applications instead of one, but again I would defer in the first instance to the

Department of Justice on the question whether Section 215 would in fact remove a real burden. If Section 215 is desirable, I would also consider whether DOJ wants similar authority for FISA "electronic surveillance" orders issued under 50 U.S.C. § 1805.

ENDNOTES

1. Written Testimony of David S. Kris before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security (April 28, 2005) (hereinafter Kris House Testimony). I have, of course, made that testimony available to your staff. As of this writing, it is also available at http://judiciary.house.gov/media/pdfs/kris042805.pdf.

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act or Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). Section 224 of the Patriot Act provides:

> (a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.
>
> (b) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

115 Stat. 295.

3. Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004). Section 6001 of the IRTPA provides:

> (a) IN GENERAL.—Section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) is amended by adding at the end the following new subparagraph:
>
> ''(C) engages in international terrorism or activities in preparation therefore; or''.
>
> (b) SUNSET.—The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107–56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224.

118 Stat. 3742.

4. See Kris House Testimony.

5. *In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

6. Kris House Testimony at 13.

7. Your legislative staff and the Department of Justice's Offices of Legislative Affairs and Legal Counsel would be better equipped than I am to determine the best way for Congress to express its endorsement of the Court of Review's decision. With some Justices and judges increasingly wary of legislative history, however, an enacted provision of public law may be more authoritative than even the clearest committee report or floor statement. See, *e.g.*, *Shannon* v. *United States*, 512 U.S. 573, 583 (1994) (citing cases and noting that "Members of this Court have expressed differing views regarding the role that legislative history should play in statutory interpretation").

8. Under 50 U.S.C. § 1801(e), as amended by Section 203 of the Committee's bill, the term "foreign intelligence information" would be defined as follows (with Section 203's proposed language in redline):

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect (including protection by use of law enforcement methods such as criminal prosecution) against –
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
>
> > (A) the national defense or the security of the United States; or
> >
> > (B) the conduct of the foreign affairs of the United States.

9. In my House testimony last month, I stated:

> If you decide that you want to expand DOJ's authority along these lines, and remove any statutory doubt, you should amend the definition of "foreign intelligence information" by adding the phrase "including protection against the foregoing using law enforcement methods, such as criminal prosecution," immediately after 50 U.S.C. § 1801(e)(1)(C).

Kris House Testimony at note 91 (emphasis in original). Section 203 of the bill uses almost

identical language in a slightly different place in the definition. Professor Richard Seamon, a thoughtful academic commentator in this area, has recommended a similar approach. See Richard Seamon and William Gardner, *The Patriot Act and the Wall Between Intelligence and Law Enforcement*, 28 Harv. Journal on Law and Pub. Policy 319, 458-459 (Spring 2005) (recommending an amendment to 50 U.S.C. § 1801(e)(1) to provide that foreign intelligence information means "information that relates to, and if concerning a United States person is necessary to, the ability of the United States, by law-enforcement or other lawful means, to protect against" specified threats).

For a detailed explanation of why and how this sort of amendment would function, see Kris House Testimony at 1-4, 9-12.

10. See Kris House Testimony at 12-14 & n.90.

11. I know at least one very intelligent person who disagrees. See Letter from Professor Richard Seamon to Chairman Howard Coble, House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security (May 4, 2005).

12. A full explanation for why this is the case appears on pages 9-12 of my House testimony last month. Here is an abbreviated explanation: The Court of Review interpreted Section 218 as codifying the "false dichotomy" between law enforcement methods and all other methods of protecting national security. It explained: "The government heroically tries to give [Section 218] a wholly benign interpretation. It concedes that 'the 'significant purpose' amendment recognizes the *existence* of the dichotomy between foreign intelligence and law enforcement,' but it contends that 'it cannot be said to recognize (or approve) its *legitimacy*.' Supp. Br. of U.S. at 25 (emphasis in original). We are not persuaded." *In re Sealed Case*, 310 F.3d at 734-735. On that basis, the Court of Review read Section 218 to permit FISA searches and surveillance primarily for law enforcement methods of protecting national security (*id*. at 734):

> as a matter of straightforward logic, if a FISA application can be granted even if 'foreign intelligence' is only a significant – not a primary – purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime.

Section 203 of the Committee's bill would eliminate the false dichotomy, and so also the premise of the Court of Review's interpretation of Section 218. To paraphrase from the block quote above, if the "foreign intelligence" purpose now includes the purpose to prosecute a target for a foreign intelligence crime (because of Section 203), then the "other purpose" that can be primary under Patriot Act Section 218 would have to be something different than prosecuting a target for a foreign intelligence crime – and indeed, different than anything that protects national security. Allowing FISA to be used primarily for something other than a "foreign intelligence" purpose (once "foreign intelligence" has been defined to include prosecution) seems unnecessary and unwise.

13. Testimony of Gregory T. Nojeim, Associate Director and Chief Legislative Counsel Washington Legislative Office, American Civil Liberties Union, before the Subcommittee on Crime, Terrorism and Homeland Security of the House Judiciary Committee (April 28, 2005) (available at http://judiciary.house.gov/media/pdfs/nojeim042805.pdf).

14. 18 U.S.C. §§ 2510-2522.

15. A Title III application must contain "details as to the particular offense that has been, is being, or is about to be committed." 18 U.S.C. § 2518(1)(b)(i). To grant the application, the court must find "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter." 18 U.S.C. § 2518(3)(a). These provisions apply to all Title III cases, roving and non-roving.

16. See note 15, *supra*.

17. A Title III application must include "the identity of the person, if known, committing the [specified] offense and whose communications are to be intercepted." 18 U.S.C. § 2518(1)(b)(iv) (emphasis added). To grant the application, the court must find probable cause that "an individual is committing, has committed, or is about to commit a particular [specified] offense." 18 U.S.C. § 2518(3)(a) (emphasis added). In keeping with these provisions, the Supreme Court has held that "when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a [non-roving] wire interception order may, nevertheless, properly issue under the statute." *United States* v. *Kahn*, 415 U.S. 143, 157 (1974).

18. A Title III application in a non-roving case must include "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii). To grant the application, the court must find probable cause either (1) that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of [the specified] offense," or (2) that those facilities or places are "leased to, listed in the name of, or commonly used by [the] person" committing the specified offense. 18 U.S.C. § 2518(3)(d). However, the Department of Justice has publicly revealed that "[f]or prudential reasons," it is "often cautious about using the 'listed, leased, or commonly used' provision of Title III absent evidence that the facility is in fact being used in connection with the predicate offense." Supplemental Brief for the United States in *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), at 18 n.6.

19. To obtain Title III roving surveillance authority for oral communications, the government must "identif[y] the person committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(11)(a)(ii). To obtain Title III roving surveillance authority for wire and electronic communications, the government must "identif[y] the person believed to be committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(11)(b)(ii).

20. Under 18 U.S.C. § 2518(11), the requirements of 18 U.S.C. §§ 2518(1)(b)(ii) and (3)(d), discussed in note 18, *supra*, "do not apply" if the government meets the other requirements for Title III roving surveillance of oral, wire, or electronic communications.

21. Here is the description of roving Title III surveillance authority from the United States Attorneys' Manual (§ 9-7.111):

> Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. See *United States* v. *Bianco*, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994); *United States* v. *Orena*, 883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications will be intercepted when it can be shown that the subject or subjects of the interception have demonstrated a purpose to thwart interception by changing facilities. See *United States* v. *Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States* v. *Petti*, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 113 S. Ct. 1859 (1993); *United States* v. *Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993).

22. Under Title III, the term "oral communication" means "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(4). Oral communications would be intercepted by, *e.g.*, a concealed microphone.

23. 18 U.S.C. § 2518(11)(a). Section 2518(11)(a) provides:

> The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if –
>
> > (a) in the case of an application with respect to the interception of an oral communication –
> >
> > > (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General,

> an Assistant Attorney General, or an acting Assistant Attorney General;
>
> (ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
>
> (iii) the judge finds that such specification is not practical.

24. 18 U.S.C. § 2518(12). The legislative history of this provision explains with respect to this "ascertainment" language:

> Proposed subsection 2518(12) of title 18 provides * * * that where the federal government has been successful in obtaining a relaxed specificity order, it cannot begin the interception until the facilities or place from which the communication is to be intercepted is ascertained by the person implementing the interception order. In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation. * * * This provision puts the burden on the investigation agency to ascertain when the interception is to take place.

S. Rep. No. 99-541, 99th Cong., 2d Sess. 32 (Oct. 17, 1986) (hereinafter ECPA Senate Report).

25. Under Title III, the term "wire communication" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." 18 U.S.C. § 2510(1). Under Title III, a telephone call is a wire communication.

26. Under Title III, the term "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12). Under Title III, an electronic mail message is an electronic communication.

27. 18 U.S.C. § 2518(11)(b)(ii)-(iii). Section 2518(11) provides:

> The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if –
>
> * * * *
>
> (b) in the case of an application with respect to a wire or electronic communication –
>
> (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
>
> (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;
>
> (iii) the judge finds that such showing has been adequately made; and
>
> (iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

28. 18 U.S.C. § 2518(11)(b)(iv). Under 18 U.S.C. § 2518(12), "[a] provider of wire or electronic communications service that has received [a roving surveillance order] may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion."

29. A FISA application for electronic surveillance must include "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. § 1804(a)(3).

30. A FISA application for electronic surveillance must include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that – (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(A). To grant the FISA application, the Foreign Intelligence Surveillance Court

(FISC) must find, "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that – (A) the target of the surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(A).

31. See 50 U.S.C. § 1801(a)-(b) (defining "foreign power" and "agent of a foreign power").

32. A FISA application for electronic surveillance must include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that * * * (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(B). To grant the FISA application, the FISC must find, "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that * * * (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B).

33. The certification that is part of every FISA application must designate the type of foreign intelligence information being sought by the electronic surveillance, and explain the basis for the designation. 50 U.S.C. § 1804(a)(7)(D) and (E)(i).

34. 50 U.S.C. § 1805(c)(2)(B).

35. See note 32, *supra*.

36. As discussed in notes 18 and 32, *supra*, the government normally satisfies Title III by establishing probable cause that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of [the underlying] offense," 18 U.S.C. § 2518(3)(d), and FISA requires probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B).

37. ECPA Senate Report at 31.

38. 50 U.S.C. § 1805(c)(1)(B).

39. 50 U.S.C. § 1805(a)(3)(B).

40. 50 U.S.C. § 1801(h)(1).

41. The nexus requirement applies only to each facility at which surveillance "is" directed, but the use of the present tense plainly would not support an argument that roving surveillance – which occurs in the future – is exempt from the requirement. On the contrary, even in an ordinary (non-roving) FISA case, the surveillance commences in the future – i.e., after the FISC has issued its order.

42. 18 U.S.C. § 2518(11)(b)(iv).

43. Roving FISA surveillance is in fact being done. The Department of Justice revealed that there had been 49 roving FISA surveillance orders issued as of March 30, 2005. Testimony of James A. Baker, Counsel for Intelligence Policy, before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, United States House of Representatives, April 28, 2005 (available at http://judiciary.house.gov/media/pdfs/baker042805.pdf) (hereinafter Baker House Testimony).

The Department supports roving FISA surveillance with arguments similar to, but not identical to, the ones I advance here. As James Baker, the Counsel for Intelligence Policy, testified on April 28, 2005:

> Let me respond to this criticism [concerning "John Doe" warrants] in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C. § 1805(c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of irrelevant communications of innocent Americans. Both the Attorney General and the FISA Court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans.

Baker House Testimony at 2 (emphasis in original).

44. See 50 U.S.C. § 1805(f).

45. Under 50 U.S.C. § 1801(b)(1)(A), an "agent of a foreign power" is defined to include

> (1) any person other than a United States person, who –
>
> > (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section.

Under 50 U.S.C. § 1801(a)(4), a "foreign power" is defined to include "a group engaged

in international terrorism or activities in preparation therefor."

Under 50 U.S.C. § 1801(c), "international terrorism" is defined to mean activities that

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended –
>
> > (A) to intimidate or coerce a civilian population;
> >
> > (B) to influence the policy of a government by intimidation or coercion; or
> >
> > (C) to affect the conduct of a government by assassination or kidnapping; and
>
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

46. Under 50 U.S.C. § 1801(b)(2), an "agent of a foreign power" is defined to include:

> any person who –
>
> > (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> >
> > (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> >
> > (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> >
> > (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United

> States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

47. See 50 U.S.C. §§ 1805(e)(1)(B), (e)(2)(B) (electronic surveillance), 1824(d)(1)(B), (d)(2)(B) (physical searches).

48. See 50 U.S.C. §§ 1810 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover" money damages); 1828 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A), respectively, of this title, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 1827 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover" money damages).

49. See 50 U.S.C. §§ 1801(b)(1)(A), 1805(e)(1)(B). FISA's legislative history explains that the "term 'member' means an active, knowing member of the group or organization which is a foreign power. It does not include mere sympathizers, fellow-travelers, or persons who may have merely attended meetings of the group or organization." H.R. Rep. No. 1283, Part I, 95th Cong., 2d Sess. 34 (1978) (hereinafter House Report) This is, of course, a fact-intensive inquiry.

50. 50 U.S.C. §§ 1805(e)(1)(B), (2)(B), 1824(d)(1)(B), (d)(2)(B); see 50 U.S.C. § 1801(b)(1)(A).

51. 50 U.S.C. § 1801(n) ("'Contents', when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication").

52. 18 U.S.C. § 2510(8) ("'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication").

53. See House Report at 51 (stating that pen registers were intended to be included in the definition of "electronic surveillance" in 50 U.S.C. § 1801(f)(2)), 67 ("devices such as pen registers are included"); see also S. Rep. No. 185, 105th Cong., 2d Sess. 27 (1998) (noting that pen registers were considered electronic surveillance under the original version of FISA) (hereinafter Senate Intelligence Pen-Trap Report).

54. Pub. L. No. 105-272, § 601, 112 Stat. 2396 (Oct. 20, 1998), codified at 50 U.S.C. §§ 1841-1846. Pen-trap orders may be obtained on a lesser showing than would be necessary for electronic surveillance or a physical search because the Supreme Court has held that limited information concerning the source or destination of a communication is not protected by the Fourth Amendment. See *Smith v. Maryland*, 442 U.S. 735 (1979). The Court in *Smith* reasoned that a person does not have a reasonable expectation of privacy in the numbers dialed from a telephone and therefore that a pen register does not constitute a "search" within the meaning of the Fourth Amendment. *Id.* at 742-46. Absent the statutory requirements to obtain a court order, therefore, the government could employ pen-trap devices without any judicial authorization.

55. See 50 U.S.C. § 1841(2) (defining pen register and trap and trace by reference to 18 U.S.C. § 3127).

56. 18 U.S.C. § 3127(3).

57. See note 62, *infra*.

58. 18 U.S.C. § 3127(4).

59. See www.usdoj.gov/criminal/cybercrime/PatriotAct.htm. A trap and trace device is still defined in the statute as a trap and trace "device" even if it is in fact a process, rather than a device.

60. See *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electronic impulses caused when the dial on the phone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").

61. See U.S. Internet Service Provider Association, *Electronic Evidence Compliance – A Guide for Internet Service Providers*, 18 Berkeley Tech. L. J. 945, 956 (2003) ("Law enforcement may also use pen register and trap and trace orders to trace communications on the Internet and other computer networks."). Prior to the Patriot Act, pen registers had been used to obtain computer routing and addressing information, but it was not well settled that this was the correct interpretation of the statute. See www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.

62. 18 U.S.C. § 3127(3) & (4). FISA does not incorporate a provision of the criminal code that requires the government to use "technology reasonably available to it that restricts" pen-trap interceptions "so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c). However, Section 2.4 of Executive Order 12333 imposes similar restrictions, requiring Intelligence Community agencies, which include the intelligence elements of the FBI, to "use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."

63. It applies only to the subchapter of FISA regulating electronic surveillance. Under the first sentence of 50 U.S.C. § 1801, the definitions in that section apply only to "this title," or Title I of

FISA. The pen-trap provisions are in Title IV of FISA. Although Congress chose to incorporate by reference into the FISA pen-trap provisions many of the definitions applicable to electronic surveillance, it did not incorporate FISA's definition of "contents." See 50 U.S.C. § 1841.

64. 50 U.S.C. § 1801(n).

65. There may, of course, be another reason for Section 202, but if so I am unaware of it.

66. One other concern might arise from 18 U.S.C. § 2511(2)(f), which provides in relevant part that "procedures in [Title III] or [the Stored Communications Act, 18 U.S.C. §§ 2701-2712] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as described in [50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted." FISA's broad definition of "contents" means that its definition of "electronic surveillance" is correspondingly broad, see 50 U.S.C. § 1801(f)(1)-(3), and includes pen-trap surveillance. This might give rise to the concern that Section 2511(2)(f) forbids criminal pen-trap surveillance because it provides that FISA and Title III are the "exclusive means" for conducting such surveillance. In other contexts, however, the courts of appeals have rejected arguments that Section 2511(2)(f) forbids domestic law enforcement investigative conduct that is "electronic surveillance" under FISA but not under Title III. See, *e.g.*, *United States* v. *Koyomejian*, 970 F.2d 536. 540-541 (9th Cir. 1992) (en banc) (silent video surveillance, which is "electronic surveillance" as defined by FISA but is not regulated by Title III, may be conducted against domestic, criminal targets without following either FISA or Title III). This is a very complex area, in which I may not know all the relevant facts, but in any event, my sense is that if an amendment is needed, the provision to be amended should be 18 U.S.C. § 2511(2)(f), not FISA.

67. See 50 U.S.C. § 1841(2) (FISA pen-trap devices defined by cross-reference to criminal pen-trap statute), 18 U.S.C. § 3127(3)-(4) (criminal pen-trap surveillance may not intercept "contents"), 18 U.S.C. § 3127(1) (defining "contents" for criminal pen-trap statute by cross-reference to Title III), 18 U.S.C. § 2510(8) (defining "contents" in Title III as "any information concerning the substance, purport, or meaning of [a] communication").

68. 18 U.S.C. § 2510(8).

69. See Electronic Communications Privacy Act (ECPA), Pub. L. 99-508, § 101(a)(5), 100 Stat. 1848, amending 18 U.S.C. § 2510(8); see also ECPA Senate Report at 13-14.

70. 50 U.S.C. §§ 1842(a)(1), (a)(2).

71. As a technical drafting matter, the bill should specify that the change pertains to the second use of the word "for" in the provision.

72. There are similar First Amendment provisions in other parts of FISA. See 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A) ("no United States person may be considered * * * an agent of a foreign power solely upon the basis of activities protected by the first amendment to the

Constitution of the United States"). (The electronic surveillance version of this standard applies to foreign powers and agents of foreign powers; the physical search version applies only to agents of foreign powers. I doubt the omission was intentional.) See also 50 U.S.C. §§ 1842(a)(1), (c)(2), 1843(a), (b)(1) (similar provisions for pen-trap surveillance).

73. 50 U.S.C. § 1861(d).

74. 334 F. Supp.2d 471 (S.D.N.Y. 2004).

75. 18 U.S.C. § 2709. Section 2709 provides that "[a] wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation." 18 U.S.C. § 2709(a). It also provides that "[n]o wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section." 18 U.S.C. § 2709(c).

76. 334 F. Supp.2d at 514.

77. *Id*.

78. The Department of Justice is apparently of the same view. See Baker House Testimony at 3-4 ("some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points.").

79. See, *e.g.*, *Los Angeles Police Dep't* v. *United Reporting Publishing Co.*, 528 U.S. 32, 37-39 (1999) (explaining First Amendment overbreadth doctrine); cf. *United States* v. *Salerno*, 481 U.S. 739, 745 (1987) ("The fact that [a statute] might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid, since we have not recognized an 'overbreadth' doctrine outside the limited context of the First Amendment").

80. See, *e.g.*, Executive Order 12958 (as amended).

81. See, *e.g.*, *Snepp* v. *United States*, 444 U.S. 507, 510 n.3 (1980).

82. 50 U.S.C. §§ 1801(h), 1805(a), 1805(c)(2)(A), 1821(4), 1824(a), 1824(c)(2)(A).

83. Executive Order 12333 § 2.3; see also *id*. § 1.14. The intelligence elements of the FBI are in the intelligence community. *Id*. § 3.4(f)(6).

84. Baker House Testimony at 3 ("The Attorney General also recently declassified the fact that the FISA Court has issued 35 orders under section 215 from the effective date of the Act through March 30th of this year. The Attorney General also declassified the types of business records sought by these orders. They include driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices. None of those orders were issued to libraries and/or booksellers, or were for medical or gun records.").

85. I have not reviewed Section 212 word-by-word against the current postal regulations.

86. I was recently made aware of a November 19, 2004 letter from Attorney General Ashcroft to the Postmaster General, in which the Attorney General asked the Postmaster General to amend the mail regulations. The requested changes were not made.

87. Compare 39 C.F.R. § 233.3(c)(1)(i) and (9)(i)-(iii), with 50 U.S.C. § 1801(e)(1).

88. 39 C.F.R. § 233.3(c)(3)(8).

89. 39 C.F.R. § 233.3(e)(3).

90. 39 C.F.R. § 233.3(e)(2)(i).

91. 39 C.F.R. § 233.3(g)(5)-(6).

92. 39 C.F.R. § 233.3(g)(8).

93. Under 39 U.S.C. § 201, the Postal Service is "an independent establishment of the executive branch." For a discussion of the status and corporate governance structure of the Postal Service, see *United States Postal Service* v. *Flamingo Industries (USA) Ltd.*, 540 U.S. 736, 740 (2004).

94. The current guidelines for national security investigations issued under Executive Order 12333 are classified in part. See www.usdoj.gov/olp/nsiguidelines.pdf and www.usdoj.gov/olp/nsifactsheet.pdf. An earlier version of these guidelines, issued in May 1995, is also classified in part. See www.usdoj.gov/ag/readingroom/terrorismintel2.pdf.

95. 50 U.S.C. §§ 1861-1862.

96. 18 U.S.C. § 3486.

97. 21 U.S.C. § 876 ("In any investigation relating to his functions under this subchapter with respect to controlled substances, listed chemicals, tableting machines, or encapsulating machines, the Attorney General may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the Attorney General finds relevant or material to the investigation."). For what appears to be a truly comprehensive list of

administrative subpoena authorities held by Executive Branch entities, see United States Department of Justice, Office of Legal Policy, *Appendices A, B & C Accompanying Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities Pursuant to Public Law 106-544*, available at www.usdoj.gov/olp/appendixa1.pdf, www.usdoj.gov/olp/appendixa2.pdf, www.usdoj.gov/olp/appendixb.pdf, and www.usdoj.gov/olp/appendixc.pdf.

98. See United States Department of Justice, Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities Pursuant to Public Law 106-544*, Table I at 40-41, available at http://www.usdoj.gov/olp/intro.pdf (hereinafter DOJ Administrative Subpoena Report).

99. Between October 26, 2001, and January 21, 2003, the FBI issued what appears to be several hundred national security letters, although the precise number is apparently classified. See www.aclu.org/patriot_foia/FOIA/NSLLists.pdf.

100. DOJ Administrative Subpoena Report at 41 (noting delegation from Attorney General to FBI Director of authority to issue subpoenas under 18 U.S.C. § 3486 in investigations of child sex abuse).

101. See Kris House Testimony at 16-18.

102. See 50 U.S.C. § 1808(a)(2)(A) (semi-annual report shall describe "each criminal case in which information acquired under this Act has been passed for law enforcement purposes during the period covered by such report"). See also 50 U.S.C. § 1806(b) ("No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.").

103. Under 50 U.S.C. § 1808(a)(2)(B), the semi-annual report must include a description of "each criminal case in which information acquired under this chapter has been authorized for use at trial during such reporting period."