David S. Kris
800 Connecticut Avenue, NW
Suite 800
Washington, DC 20006

May 1, 2007

The Honorable John D. Rockefeller IV
Chairman
Select Committee on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman and Mr. Vice Chairman:

In response to a request from your staff, I am writing with my comments on the Foreign Intelligence Surveillance Modernization Act of 2007, which I understand was submitted to Congress by the executive branch as proposed Title IV of the Intelligence Authorization Act for Fiscal Year 2008. The proposal is 66 pages long and includes several very significant changes to the Foreign Intelligence Surveillance Act (FISA). Although I have had ample time to consider the meaning of current FISA, my comments on the government's proposal are the product of a very few days, and are necessarily tentative.[1]

I have three general reactions to the government's proposal. First, with few exceptions (changes to the definition of "agent of a foreign power"), it does not expand the range or type of surveillance that the government may lawfully conduct. In other words, it is not primarily designed to fill any gaps in available coverage. In any event – and this is my second reaction – the proposal substantially shifts the power to authorize surveillance from the judicial to the executive branch. In other words, it contracts the jurisdiction of the Foreign Intelligence Surveillance Court (FISC), and expands the authority of the Attorney General and the National Security Agency (NSA). Third and finally, I worry that this proposal may have unintended consequences in a statute as complex as FISA (although I concede that I have not had much time to review the proposal or to consider the ways in which its various elements work together).

In my opinion, Sections 401(b) and 402 are by far the most significant provisions in the government's proposal. I focus much of my attention on them. Where possible, however, I also discuss other provisions in the proposal. Following a brief summary of my views, which is set out immediately below, I try to describe and explain the law as it is today, and then address how I believe the law will change if the government's proposal is enacted. I do not significantly confront the policy arguments for or against the government's proposal; in part because of time constraints, my main purpose now is to *explain* what I think it means.

SUMMARY

Section 401(a). Section 401(a) of the government's proposal would amend the definition of "agent of a foreign power" in FISA to include any non-U.S. person who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States," if the government certifies that the foreign intelligence information is "significant." This provision appears to me to be a catch-all, and the Committee may want the government to identify one or more real or hypothetical cases to justify it. I would not be surprised if such examples can only be provided in closed session. Assuming the provision is needed, I believe the Committee should consider carefully what it means for "foreign intelligence information" to be "significant," and consider how that adjective will work with the current syntax of the definition. Finally, because this provision merges the probable-cause and purpose provisions of the statute, I also believe the Committee should consider limiting its use to situations in which the government cannot satisfy the other definitions of "agent of a foreign power."

Section 401(b). Section 401(b) of the government's proposal would amend the definition of "electronic surveillance," on which the entire regulatory framework of subchapter I of FISA depends. This is major surgery on a very complex statute, and it may well be necessary, but it definitely should not be undertaken lightly. I have tried, in the body of this letter, to review extremely carefully the meaning of current FISA, the ways in which that meaning will change if the government's proposal is enacted, and the implications of such change for various forms of actual surveillance activity. But I am four years out of government, and national security is just my hobby. The Committee may want to request a far more authoritative and comprehensive analysis from the executive branch, to help explain *exactly* how the government's proposal will affect surveillance operations, and protections for privacy and civil liberties, as well as the reasons why change is needed or desired. This is an area in which the tiniest technical details can make an enormous difference.

I have three specific questions about Section 401(b). First, what does it mean to "intentionally direct[] surveillance at a *particular, known* person" under proposed Subsection (1) of the definition of "electronic surveillance"? In particular, does this language exclude wide-ranging or "driftnet" surveillance, on the theory that the target of such surveillance is *all* persons (or persons in general), rather than any "particular, known" person? If not, what does the government say to changing the language to refer to "any person or persons" instead of a "particular, known person"?

Second, why does proposed Subsection (1) refer to the reasonable expectation of privacy enjoyed by "that person" – the "particular, known" target of the surveillance – rather than the traditional formulation, "a person"? What is the government's view on whether foreign governments and non-U.S. persons enjoy Fourth Amendment rights while inside the United States? How will the use of "that person" affect surveillance of them?

Third, although I cannot discuss them here, there are several technically complex – and arguably metaphysical – questions about the application of this provision to e-mail. The Committee may want to discuss this with the government in a closed session.

Section 402. Section 402, which would amend 50 U.S.C. § 1802, is also a far-reaching proposal. It authorizes surveillance of certain foreign powers without judicial review. In 1978, the absence of judicial review was justified by the fact that the provision governed "a class of surveillances, otherwise within the scope of the bill, where there was little or no likelihood that Americans' Fourth Amendment rights would be involved in any way."[2] Under the government's proposal, that would no longer be the case. Thus, the main policy question is relatively clearly presented.

Congress should also request a more complete explanation of proposed 50 U.S.C. § 1802A, which would also be enacted by Section 402 of the government's proposal. How does this provision relate to the narrowing of the definition of "electronic surveillance" in Section 401(b) of the proposal? How, if at all, would it affect the (judicial or non-judicial versions of) the Terrorist Surveillance Program (TSP) and other existing or contemplated surveillance programs? Finally, are one-year periods of unilateral executive branch surveillance of U.S. persons "reasonable" under the Fourth Amendment?

Section 404. The most significant aspect of Section 404 of the government's proposal is that it allows the President to name *any* federal officer as the certifying official for a FISA application. Under current law, only a Senate-confirmed official may be named. This is an important change because, while it offers obvious operational benefits, it risks denigrating the significance of the certification.

DISCUSSION

The following paragraphs present my comments on current law, and the government's proposal, in more detail. **For ease of reference, given the length and density of the discussion, I have presented what I think are the most important points in bold text.**

Section 401(a)

Section 401(a) of the government's proposal would amend the definition of "agent of a foreign power" in FISA to include any non-U.S. person who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States," if the government certifies that the foreign intelligence information is "significant."

1. Background on Current FISA's Basic Requirements.

To understand Section 401(a), it is necessary to review two aspects of FISA as it stands today. First, under current law, every FISA application for electronic surveillance or a physical search must include a statement of facts that is "relied upon by the applicant to justify his belief,"[3] and used by the FISC to determine probable cause, that the target of the surveillance or search is a "foreign power" or an "agent of a foreign power."[4] This is often referred to as the statute's probable-cause requirement.

Second, every FISA application today must also contain a certification, by a high-ranking executive branch official, that the information sought is "foreign intelligence information" and that a significant purpose of the search or surveillance is to obtain "foreign intelligence information" – a term that is defined to include information that is relevant or necessary to the ability of the United States to protect against various specified foreign threats to national security, including attack, sabotage, international terrorism, and espionage.[5] This is often referred to as the statute's purpose requirement.

Together, the probable-cause and purpose requirements are the fundamental limit on (and justification for) the use of FISA. They distinguish the statute from other information-gathering techniques used in other contexts, such as wiretapping in ordinary criminal investigations under Title III.[6]

2. FISA's Definition of "Agent of a Foreign Power."

Both "foreign power" and "agent of a foreign power" are defined in great detail in current Section 1801 of FISA.[7] Broadly speaking, a "foreign power" is an entity, such as a nation or an organization, including an international terrorist group,[8] and an "agent of a foreign power" is an individual who is in some way affiliated with a foreign power, such as a member of an international terrorist group.[9] Under current law, the only exception to that general rule of affiliation is the so-called "lone wolf" provision of FISA, which states that a non-U.S. person may be an "agent of a foreign power" if he "engages in international terrorism or activities in preparation therefor[]," regardless of whether he has a relationship with a terrorist group.[10] As I understand it from the government's public statements, the lone-wolf provision was designed to reach cases where (1) an individual genuinely is acting alone, perhaps inspired by, but not actively working for, an international terrorist group; or (2) the individual is indeed working for an international terrorist group, but the government cannot establish probable cause of that fact. In an era of widespread, ideologically-driven international terrorism, and proliferating nuclear weapons that fit inside carry-on luggage, this provision makes sense.

Section 401(a) of the government's proposal would expand on the rationale underlying the lone-wolf provision by creating what amounts to a catch-all provision for non-U.S. persons. Under this provision, if the government reasonably believes that the non-U.S. person has foreign intelligence information, the person is an agent of a foreign power and may be targeted. In other words, Section 401(a) effectively merges the statute's probable-cause and certification requirements.

3. FISA's Definition of "Foreign Intelligence Information."

Section 401(a) requires the "foreign intelligence information" sought under the catch-all provision to be "significant." I am not sure what that would mean. Current FISA contains five separate, but overlapping, definitions of "foreign intelligence information," divided into two sets. The first set defines "foreign intelligence information" in terms of protecting against various foreign threats to the national security.[11] This is sometimes referred to as protective foreign intelligence. The first set of definitions provides:

> Foreign intelligence information means –
>
> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> (A) actual of 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 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[12]

The second set of definitions relates to the executive branch's need for affirmative foreign intelligence information to conduct foreign relations and make foreign policy decisions. This is sometimes referred to as affirmative foreign intelligence. This second set of definitions provides that foreign intelligence information also means –

> (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.[13]

As these definitions make clear, apart from being divided into two sets – protective and affirmative intelligence – "foreign intelligence information" is also defined under two standards. Information "concerning a United States person" (e.g., a citizen or lawful permanent resident alien) may be foreign intelligence information only if it is "necessary" to the goal it serves (e.g., the ability of the United States to protect against international terrorism). By contrast, information concerning a non-U.S. person may be foreign intelligence information if it is merely "relevant" to that goal.

Congress imposed the "necessary" standard to protect the privacy of United States persons "from improper activities by [U.S.] intelligence agencies" while also protecting the United States and its allies "from hostile acts by foreign powers and their agents."[14]

"Necessary," according to the 1978 House Report, means that the information "is both important and required," not just that its collection would be "useful and convenient"; the government must show a "significant need" for the information.[15] Although the House Report acknowledges that the term "necessary" could encompass "every possible bit of information about a subject because it might provide an important piece of the larger picture," it explains that "such a reading is clearly not intended."[16]

The difference between "necessary" and "relevant" may prove elusive. For example, investigators may find it difficult to determine, especially at the early stages of an investigation, whether information concerning a U.S. person is actually necessary to protect against terrorism or instead merely "relates to" that goal. The House Report itself reflects this problem of interpretation. Although the Report disapproves a broad view of "foreign intelligence information" that would encompass information "about a U.S. person's private affairs," the Report suggests that such information constitutes foreign intelligence information if "it *may* relate to his activities on behalf of a foreign power."[17] As a practical matter, moreover, personal information about spies and terrorists is nearly always arguably "necessary" to the protection of national security, because knowledge of the movements, habits, and preferences of these individuals may be crucial in thwarting threats to the national security.[18]

By referring to "significant" foreign intelligence information, does Section 401(a) mean to apply the U.S.-person standard – "necessary" – to information that, in most cases, will be "concerning" a non-U.S. person and therefore otherwise subject to the "relevant" standard?[19] I don't know. The "significant" adjective seems to reflect the government's sense that this provision should not be used except in important cases. It may be better, however, to express that sense through the existing syntax of FISA's definition of foreign intelligence information. It also may be wise explicitly to limit the use of this provision to cases where the government affirms that it cannot satisfy the other definitions of "agent of a foreign power" in FISA.

Section 401(b)

Section 401(b) of the government's proposal would amend FISA's definition of "electronic surveillance." This would be a very significant change in the law. It should be the hard center of any attention that is paid to this proposal. Unfortunately, to understand the government's proposal, it is necessary first to understand current law, and current law is enormously complex. In the discussion that follows, I try to explain the importance of the definition of "electronic surveillance" to the regulatory scheme established by FISA (part 1); provide an overview (part 2), a detailed analysis (part 3), and a description of the limits (part 4) of the current definition of "electronic surveillance; explain the definition of "physical search" in current FISA, because it intersects directly with the definition of "electronic surveillance" (part 5); and explain how the definitions apply to various forms of real-world surveillance (part 6). I then try to do the same for the government's proposed new definition of "electronic surveillance" (part 7), and discuss how the proposed definition may intersect with Title III (part 8).

1. Background on the Significance of "Electronic Surveillance" as Defined by FISA.

FISA authorizes and regulates "electronic surveillance" by the government in certain circumstances, and the scope of the authorization and regulation depends largely on the meaning of that term. For example, the FISC has jurisdiction to hear applications for and grant orders approving "electronic surveillance" anywhere within the United States under the procedures set forth in FISA.[20] Those procedures generally require the government to submit an application for an order approving "electronic surveillance,"[21] and authorize a judge of the FISC to enter an *ex parte* order approving the "electronic surveillance" if the application meets the statutory requirements.[22] The President, through the Attorney General, may authorize "electronic surveillance" without a court order under certain circumstances.[23] FISA also regulates the use of information obtained or derived from "electronic surveillance,"[24] requires certain reporting to Congress and public disclosure concerning "electronic surveillance,"[25] and provides civil and criminal penalties for anyone who engages in "electronic surveillance" under color of law except as authorized by statute.[26] **In short, the entire framework of subchapter I of FISA[27] turns on the meaning of "electronic surveillance."**

2. Overview of FISA's Current Definition of "Electronic Surveillance."

The current definition of "electronic surveillance" in FISA contains four separate subsections, and is enormously complex.[28] I therefore begin with an overview of each of the four subsections of the definition, discussing briefly the basic kinds of communications and surveillances to which each subsection applies. This is meant to serve as an orientation for the more technical discussion that follows.

The first subsection of the current definition of "electronic surveillance," 50 U.S.C. § 1801(f)(1), defines the term to mean:

> 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 provides that the government must obey FISA (e.g., by obtaining a FISC order) whenever it tries to overhear or record a telephone call or other similar communication 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[29] or a similar provision. The subsection applies equally to domestic and international communications made by U.S. persons in the United States.

The second subsection of the definition, 50 U.S.C. § 1801(f)(2), defines "electronic surveillance" to mean:

> 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. This provision is broader than the first subsection of the definition in that it applies to non-U.S. persons, such as visiting foreigners, but it is narrower in that it applies only to wire communications, not to radio communications. It also excludes a narrow band of communications of computer trespassers, who are likewise unprotected by Title III.

The third subsection of the definition, 50 U.S.C. § 1801(f)(3), defines "electronic surveillance" to mean:

> the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States.

This provision applies only to radio communications, such as CB or ham radio signals, or the signals emitted by a cordless or cellular telephone. Like the first subsection, it applies only when a law-enforcement warrant would otherwise be required for the surveillance. It also applies only when all intended parties to the radio communication are located in the United States, meaning that it does not reach international radio communications.

Finally, the fourth subsection of the definition, 50 U.S.C. § 1801(f)(4), defines "electronic surveillance" to mean:

> the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

This part of the definition applies principally to microphone surveillance rather than to traditional wiretapping. If the government installs a hidden microphone anywhere in the United States, and acquires an oral communication (rather than a telephone call), it may be governed by this provision. The same is true of video surveillance.

3. Detailed Analysis of FISA's Current Definition of "Electronic Surveillance".

A real understanding of the definition of "electronic surveillance" requires more analysis than the casual overview above. The definition, including the relationships among its four subsections, ultimately turns on six separate factors. These are the factors that must be considered when determining whether any particular act of surveillance is "electronic surveillance" as defined by FISA today.

(1) the type of information being acquired (wire communication, radio communication, or other information);

(2) the type of acquisition (e.g., through the use of a surveillance device or the installation of such a device, intentional or otherwise);

(3) the location where the acquisition occurs (inside or outside the United States);

(4) the status of the targets of the surveillance (as U.S. persons or non-U.S. persons);

(5) the location of the targets (inside or outside the United States); and

(6) the existence (or not) of a reasonable expectation of privacy and the need (or not) for a warrant to engage in the surveillance under law-enforcement rules.

In this part of my comments, I discuss each of these six factors in detail, explaining where and how each applies to the four subsections of the definition. I end this part with a summary chart describing the definition of "electronic surveillance" in terms of the six factors.

a. Type of Information or Communication.

There are three kinds of information subject to "electronic surveillance" under current FISA: wire communications,[30] radio communications,[31] and information that is neither a wire nor a radio communication.[32] FISA does not define the term "communication," but the dictionary defines it as an expression or exchange of information or ideas.[33] As such, it includes all of the following: an oral conversation, a sign-language conversation, a letter, a telegram, a telephone call, an electronic mail message, or any other form of communication that advancing technology permits.[34]

A "communication" as the term is used in FISA's definition of electronic surveillance must have a "sender" and one or more "recipients."[35] Although the statute does not make clear whether the sender and recipient of a communication can be the same person – e.g., when a person sends an e-mail from his work e-mail account to his personal e-mail account – nothing in the text or legislative history of FISA overtly conflicts with treating the same person as both sender and recipient of a communication. Similar issues may arise with respect to diaries, task lists, oral statements of persons who talk to themselves, and certain kinds of arguably "symbolic" speech.[36]

i. Wire Communication.

Two of the four parts of the current definition of "electronic surveillance" – Subsections (1) and (2) – apply to "wire communications." FISA defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[37] In keeping with the plain language of the definition, FISA's legislative history explains that communications are "wire communications" only "while they are being carried by a wire."[38] Thus, a cordless telephone call is not a wire communication while the signal travels from the handset to the base station (it is, instead, a radio communication), although the call would become a wire communication once it arrives at the base station and begins moving over a telephone line. The same logic applies to mobile telephone signals while they travel between a mobile handset and a telecommunication provider's tower; they would begin as radio communications between the handset and the tower, and would become wire communications after they arrived at the tower.[39] An e-mail message is a "wire communication" while transiting over a wire or cable, but not while transiting as a radio signal to or from a BlackBerry or other wireless e-mail device.

These distinctions can affect where and how the government may acquire a communication under current law. For example, monitoring a cordless or mobile telephone call between the handset and the base station or tower is not electronic surveillance under Subsection (2), because that provision applies only to "wire communications." As discussed below, however, it may be electronic surveillance under Subsections (1) or (3), because those provisions apply to "radio communications." Conversely, monitoring the same telephone call by tapping the telephone wires could be electronic surveillance under Subsections (1) or (2), but could not be electronic surveillance under Subsection (3), because Subsection (3) does not apply to wire communications.[40]

By restricting a "wire communication" to communications while being carried by wire, current FISA contrasts with Title III, which defines "wire communication" as "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."[41] As Congress understood when it enacted FISA, Title III's definition applies to a (wire) communication at all stages of transmission if the communication travels "in whole or in part" by wire on its journey from "the point of origin" to "the point of reception."[42]

Not all wires carry "wire communications" as defined in current FISA. Rather, the wire must be "furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[43] The common carrier must be in the business of providing interstate or international service (though of course the particular communication in question may be wholly intrastate[44]), and it must be "a U.S. common carrier and not a foreign common carrier."[45]

FISA does not define "common carrier," but the dictionary definition of the term is a "commercial enterprise that holds itself out to the public as offering to transport freight or passengers for a fee."[46] In the context of communications, rather than transportation, Title III cross-references and incorporates the federal Communications Act's definition of the term, which includes "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy, ... but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier."[47]

In part because of the cross-reference in Title III, courts might interpret current FISA's use of the term "common carrier" in accord with the Communications Act,[48] although the two statutes have very different purposes, and doing so could introduce substantial uncertainty and complexity into FISA's statutory scheme.[49] A traditional local or long-distance telephone company is the paradigmatic example of a "common carrier" under the Communications Act.[50] A mobile telephone company is also a common carrier under the Communications Act.[51] A cable television operator is not a "common carrier" under the Communications Act,[52] except insofar as it offers circuit-switched telephone service.[53] The Supreme Court has upheld the FCC's determination that "cable companies that sell broadband Internet service do not provide 'telecommunications servic[e]' as the Communications Act defines that term, and hence are exempt from mandatory common-carrier regulation."[54] Thus, if current FISA's reference to "common carrier" were interpreted in accord with the Communications Act, information (such as e-mail) being carried on a cable owned and offered by a cable modem service provider would not be a "wire communication" under FISA, and acquisition of such information would not be "electronic surveillance" under Subsections (1) and (2) of the definition. An ISP also is not a "common carrier" under the Communications Act, [55] but the telephone lines used to connect dial-up users to an ISP are usually provided by a telephone company or other common carrier.[56]

ii. Radio Communication.

Current FISA does not define the term "radio communication." As a scientific matter, radio signals are defined by their wavelength on the electromagnetic spectrum.[57] A classic example of a radio communication would be a Citizens' Band (CB) or Bluetooth signal.[58] But Congress apparently meant "radio communication" in FISA to include microwaves,[59] which may be distinguished technically from radio waves (because they have a shorter wavelength).[60] Indeed, Congress may have intended to cover the entire electromagnetic spectrum of wireless communications. The question is not authoritatively settled in publicly-available materials. Like a wire communication, however, a radio communication presumably would be a radio communication only so long as it is being carried by radio – i.e., not when the communication has left the radio waves and is transiting by wire, and not after it reaches its destination at the recipient.

iii. Information Other than Wire or Radio Communications.

The final definition of "electronic surveillance," in current Subsection (4), applies only to information acquired from sources other than wire and radio communications. This includes communications that are not carried by wire or radio, such as oral communications (acquired by

hidden microphone). It also includes non-communicative information – for example, the objects in a room, or images of a terrorist planting explosives (acquired by video cameras) – and the use of transponder devices attached to a vehicle or other object that reveal the object's location.[61]

b. Type of Acquisition.

Surveillance is "electronic surveillance" under current FISA only when the government "acquires" information.[62] FISA does not define that term, but its ordinary meaning – to gain possession of – includes not only recording and listening to a communication, but also listening to the communication without recording it, and (probably) recording it without listening to it. At least one court has held that "acquisition" as used in Title III[63] includes recording the contents of a conversation even if the recording is never listened to.[64] The same reasoning and result probably should apply to FISA recordings made and not reviewed, even if (as sometimes happens), the recordings are in fact erased without ever being heard.[65]

On the other hand, the government has in the past argued successfully under Title III (and, it appears, FISA) that the Carnivore (DCS-1000) system does not "intercept" all of the communications that pass into its programming filters.[66] Carnivore is a device that captures specified packets of data from a packet-switched computer network. To do this, Carnivore instantaneously copies into its random access memory all packets of data that are transiting the network, and then copies some of those packets to permanent memory according to its programming instructions (e.g., all packets going to a particular e-mail address on the network). The gist of the government's argument is that no interception or acquisition occurs "during all the [initial] filtering/processing" stage in which Carnivore selects the desired from the undesired packets on the monitored network, because "no FBI personnel are seeing any information – all of the information filtering/processing, and purely in a machine-readable format, is occurring exclusively 'within the box.'"[67] There may well be a reasonable distinction between the instantaneous, ephemeral "recording" of disintegrated communications in short-term electronic computer memory, and the permanent recording of integrated communications on tape or other permanent media. Essentially, the argument would be that that if the government has intercepted or otherwise enjoys meaningful access to information (including a communication), it has "acquired" that information.[68]

Acquisition is "electronic surveillance" under all four parts of the current definition only when it involves the use of an "electronic, mechanical, or other surveillance device."[69] FISA does not define that term. Title III provides that the term "electronic, mechanical, or other device" means "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," but does not include the following:

> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic

communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.[70]

The exceptions in Title III's definition – for certain telephone equipment furnished to subscribers – are more significant in that statute than in FISA because Title III generally forbids (and prescribes penalties for) interception of communications by any party, and then provides exceptions to that general prohibition for authorized surveillance by the government.[71] By contrast, FISA authorizes and regulates certain investigative activity by the government; it prescribes civil and criminal penalties only for illegal electronic surveillance conducted "under color of law."[72]

FISA's legislative history states that the use of the phrase "surveillance device" does not encompass "lock picks, still cameras, and similar devices," even though they "can be used to acquire information, or to assist in the acquisition of information."[73] By analogy to Title III's exemption for hearing aids, ordinary eyeglasses also would not be a FISA "surveillance device." The same is probably also true of "[b]inoculars, dogs that track and sniff out contraband, search-lights, fluorescent powders, automobiles and airplanes,"[74] but somewhere on the continuum between ordinary eyeglasses and sophisticated thermal imagers, items used to aid surveillance become "surveillance devices" under FISA.[75] As a practical matter, the more esoteric the technology, the more likely courts probably would be to find it a "surveillance device."[76]

There have been a number of decisions on the meaning of "surveillance device" as used in the provision of Title III making it illegal to use or possess such devices when they are designed primarily for surreptitious surveillance[77] (with many of the decisions involving cable television descramblers[78]), but these decisions often turn on the defendant's knowledge of whether the device's design makes it primarily suitable for surreptitious surveillance, and are therefore not a completely reliable guide to the meaning of "surveillance device" in FISA.[79] To be sure, the government may use its share of microphones disguised as martini olives,[80] but its authority to compel the assistance of third parties (e.g., landlords and telephone companies) means that its FISA surveillance devices need not always be designed primarily for surreptitious use.

To qualify as "electronic surveillance" under the first three subsections of FISA's current definition, a surveillance device must be used to acquire the "contents" of a communication. When used with respect to a communication, FISA defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."[81] This definition differs from Title III's definition of "contents"[82] because it includes information concerning the "existence" of a communication and the "identity of the parties" to it.[83] Thus, it effectively covers any information about a communication, including the sort of routing and addressing information (e.g., telephone numbers) acquired by pen/trap surveillance.[84] Subsection (4) is even broader, and applies to any "information" acquired, even if it is not a communication.

c. Location of Acquisition.

Two parts of FISA's current definition of "electronic surveillance," Subsections (2) and (4), apply only when the surveillance – the acquisition of the contents of the communication or the use of the surveillance device – occur inside the United States.[85] Under a separate provision of FISA, "'United States,' when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands."[86] This definition could arguably include the U.S. Naval Base in Guantanamo Bay, Cuba,[87] although the 1978 House Report on FISA states that U.S. military bases located abroad are *not* part of the "United States" when used in a geographic sense.[88] Surveillance may be "electronic surveillance" under Subsections (1) and (3) regardless of where it occurs.

d. Targets.

Under Subsection (1) of the current definition, acquisition of the contents of a wire or radio communication (using a surveillance device) is "electronic surveillance" only if the communication is "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." This provision may apply not only to FISA applications that identify a U.S. person as a target, but also to so-called "watchlisting," a process that involves monitoring a communications channel and using automated systems to intercept particular communications for review. Based on affidavits from the NSA, the D.C. Circuit has described watchlisting as follows:

> **NSA monitors radio channels. Because of the large number of available circuits, however, the agency attempts to select for monitoring only those which can be expected to yield the highest proportion of foreign intelligence communications. When the NSA selects a particular channel for monitoring, it picks up all communications carried over that link. As a result, the agency inevitably intercepts some personal communications. After intercepting a series of communications, NSA processes them to reject materials not of foreign intelligence interest. One way in which the agency isolates materials of interest is by the use of [l]ists of words and phrases, including the names of individuals and groups .... These lists are referred to as "watch lists" by NSA and the agencies requesting intelligence information from them.[89]**

In essence, watchlisting resembles a sophisticated version of using search terms to query a large database of acquired information, as is now common in pre-litigation discovery, or in legal research using Westlaw or its equivalents.[90] Under FISA, the argument would be that this kind of watchlisting – or any deliberate use of a surveillance device to monitor a specific communications channel where the but-for purpose of the surveillance is to acquire communications from a U.S. person in the U.S. – is "targeted" surveillance under Subsection (1). The only exception identified in the legislative history is where a U.S. person's communication is "acquired unintentionally."[91]

The remaining parts of the current definition – Subsections (2)-(4) – do not require targeted surveillance. In practice, of course, all FISC-authorized electronic surveillance has a "target," but the definitions mean that the government must adhere to FISA – including the requirement to designate a target and establish that it is a foreign power or an agent of a foreign power – when it conducts "electronic surveillance," even if (the government would argue) there is in fact no target, or if the target is not a U.S. person. Put another way, FISA provides that the government cannot engage in broad-brush, non-targeted surveillance as defined by Subsections (2)-(4) unless it can in fact identify a "target" and satisfy the statute's other requirements.

e. Location of Targets.

Certain parts of the current definition of "electronic surveillance" apply only where a communication's sender, recipient, or both are located in the United States. Under Subsection (1), the target of the surveillance (who may be either a sender or recipient of a communication) must be located in the United States, and under Subsection (2) either the sender or a recipient must be located in the United States. Under Subsection (3), both sender and all intended recipients must be in the United States. Under Subsection (4), the location of sender and recipient is irrelevant, but the surveillance device must be used in the United States. As discussed above, FISA defines "United States" when used in a geographic sense to include all territory under U.S. sovereignty.[92] As discussed below, difficult issues can arise when surveillance targets communications that can be sent or received from multiple locations, such as a mobile telephone call or electronic mail.

f. Reasonable Expectation of Privacy and Warrant Required for Law Enforcement.

Three of the four parts of FISA's current definition of "electronic surveillance" – Subsections (1), (3), and (4) – apply only when "a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[93] The first part of this standard – "reasonable expectation of privacy" – is a term of art from U.S. Constitutional law. It debuted in the Supreme Court in Justice Harlan's concurring opinion in *Katz v. United States*,[94] a decision holding that electronic surveillance of a telephone call is a Fourth Amendment "search." The phrase now serves as a talisman for situations in which the Fourth Amendment applies.[95]

The language of current FISA and its legislative history suggest that the reasonable expectation of privacy does not depend on the status of the individual whose privacy is being invaded by the surveillance. While Congress was considering FISA, the Department of Justice's Office of Legal Counsel "opined that foreign governments – and in some circumstances their diplomatic agents [–] have no fourth amendment rights under the Constitution."[96] The Supreme Court has stated that it is an open question "whether the protections of the Fourth Amendment extend to illegal aliens in this country."[97] Congress made clear in the legislative history that FISA's definition of "electronic surveillance" does not turn on that question. Instead, the definition depends on "the reasonableness of the expectation of privacy that a U.S. person would have with respect to [the surveillance] activity," and "is intended to exclude only those surveillances which would not require a warrant even if a U.S. citizen is a target."[98]

Although the legislative history refers to the FISA "target," the "reasonable expectation of privacy" in question should include expectations held by persons other than the FISA target or the parties to the intercepted communication (or their U.S. citizen equivalents). That follows from the statute's use of the phrase "circumstances in which *a* person" has a reasonable expectation of privacy,[99] a standard that includes any person.[100] The broader reading also makes sense in the context of FISA's physical search provisions, where the identical phrase is used.[101] If the only relevant expectation of privacy were the target's, then the FISC would have no jurisdiction[102] to authorize the physical search of a third party's home for information concerning a FISA target who was, for example, a business invitee in that home.[103]

The second part of the standard – "a warrant would be required for law enforcement purposes" – establishes a related, but different test. It is not merely an empirical test: the legislative history makes clear that "a warrant would be required for law enforcement purposes" does "not mean that a court must previously have required a warrant for the particular type of surveillance activity carried out."[104] As Congress properly understood, the executive branch may decide not to use its most effective classified intelligence collection methods in criminal cases. As a result, the surveillance "techniques involved [in FISA surveillance] may not have come before a court for a determination as to whether a warrant is required."[105] In such a situation, FISA's legislative history explains, the government should make "an assessment of the similarity with other surveillance activities which the courts have ruled upon."[106] Where an intelligence agency "wishes to use a new surveillance technique," the legislative history states that it should "seek a ruling from the Attorney General as to whether the technique requires a court order."[107] Similarly, FISC Rule 10(a)(i) provides that where the government requests "authorization to use a new surveillance or search technique," it must "submit a memorandum to the Court which: (A) explains the technique; (B) describes the circumstances of the likely use of the technique; (C) discusses legal issues apparently raised by the technique; and (D) describes proposed minimization procedures to be applied to the use of the technique."[108]

Surveillance is "electronic surveillance" under current Subsections (1), (3), and (4) only when both conditions are met – that is, only when there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[109] There are situations in which a reasonable expectation of privacy exists, but no warrant is required – for example, a search (including electronic monitoring) pursuant to consent,[110] a search incident to arrest,[111] the search of a car,[112] and an inventory search.[113] Conversely, as discussed in more detail below, there are situations in which a warrant is clearly required but there may be no reasonable expectation of privacy (at least as held by the target of the surveillance or search),[114] and other situations in which there is clearly no reasonable expectation of privacy but a warrant may be required.[115]

In the USA PATRIOT Act,[116] Congress carved out surveillance of computer trespassers from the definition of "electronic surveillance" in current Subsection (2) by cross-referencing a provision of Title III, 18 U.S.C. § 2511(2)(i).[117] Under that provision of Title III, the government may conduct surveillance of a hacker's wire or electronic communications[118] on a computer, with the consent of the computer's owner, if those communications are relevant to a lawful investigation and the surveillance acquires only communications to or from the hacker. This provision may not be necessary in most situations: if a trespasser's transmission of electronic hacking tools to a victim's protected computer is a "wire communication" under FISA,

as it must be to fall within Subsection (2), then the victim will usually (but perhaps not always[119]) be a "party thereto," whose consent removes the surveillance from Subsection (2) regardless of Section 2511(2)(i). Subsection (2) is, however, the only part of FISA's definition of "electronic surveillance" that does not explicitly state that "a warrant would be required for law enforcement purposes," and so the cross-reference may be understandable as an act of caution in a difficult statutory matrix.

g. Chart.

The following chart presents the four subsections of FISA's current definition of "electronic surveillance" in terms of the six factors discussed above.

Statute	50 U.S.C. § 1801(f)(1)	50 U.S.C. § 1801(f)(2)	50 U.S.C. § 1801(f)(3)	50 U.S.C. § 1801(f)(4)
Type of communication	Wire or radio	Wire	Radio	Non-wire, non-radio
Type of Acquisition	Acquisition of contents by electronic, mechanical, or other surveillance device	Acquisition of contents by electronic, mechanical, or other surveillance device	Intentional acquisition of contents by electronic, mechanical, or other surveillance device	Installation or use of electronic, mechanical, or other surveillance device for monitoring to acquire information
Location of Acquisition	No geographical limit on acquisition	Acquisition must occur in the U.S.	No geographical limit on acquisition	Device must be used in the U.S.
Targets	Sent by or intended to be received by a particular, known U.S. person who is intentionally targeted	To or from a person	No limit on persons (all persons)	No limit on persons (all persons)
Location of Targets	Targeted U.S. person must be in the U.S.	Communication must be to or from a person in the U.S.	Sender and all intended recipients must be located in the U.S.	No limit on location of persons (all places)
Reasonable Expectation of Privacy (REP) and Warrant Required for Law Enforcement (LE) Purposes	A person has a REP and warrant required for LE purposes	Without consent of any party to the communication, not including trespassers as defined in 18 U.S.C. § 2511(2)(i)	A person has a REP and warrant required for LE purposes	A person has a REP and warrant required for LE purposes

4. Limits in FISA's Current Definition of "Electronic Surveillance."

It may be helpful to review the limits in the current definition of "electronic surveillance" – i.e., surveillance activity that is not "electronic surveillance" under current FISA, and therefore is not regulated by FISA today. There are four important limits.

First, the statute does not apply where all parties to a communication are located abroad. Purely foreign communications are simply beyond FISA's ambit.[120] That is the case regardless of the type of communication (wire or oral), the type of acquisition, the location of acquisition (inside or outside the U.S.), the parties' status as U.S. persons or targets, and any person's expectation of privacy. That is because Subsections (1)-(3) of the definition each require at least one party to a communication to be located in the United States,[121] and Subsection (4) does not apply outside the U.S.[122]

Second, FISA does not apply where the target is located abroad, and the surveillance (acquisition) occurs abroad, regardless of any other statutory factor.[123] Where the target is abroad, Subsections (1) and (3) do not apply; and where the acquisition occurs abroad, Subsections (2) and (4) do not apply. Surveillance conducted abroad, targeting U.S. persons located abroad, is regulated under Section 2.5 of Executive Order 12333 and the Fourth Amendment. As FISA's legislative history explains, the statute "does not afford protections to U.S. persons who are abroad," and "does not bring the overseas surveillance activities of the U.S. intelligence community within its purview."[124]

Third, FISA does not apply to wire surveillance not targeting a U.S. person if the surveillance (acquisition) occurs abroad, regardless of any other statutory factor. This kind of surveillance may intercept wire communications to or from U.S. persons in the United States – e.g., if a U.S. person calls (or is called by) a surveillance target located abroad whose calls are being acquired abroad. Again, however, a U.S. person located in the U.S. cannot be the *target* of the surveillance without triggering Subsection (1), even if the surveillance (acquisition) occurs abroad.

Fourth and finally, FISA does not apply to radio surveillance not targeting a U.S. person where any party to the radio communication is outside the United States, regardless of any other statutory factor. It may be that some radio communications cannot be the subject of "electronic surveillance" because, to the extent that they are omni-directional signals easily intercepted by the general public, they do not generate a reasonable expectation of privacy.[125] To the extent that there is a reasonable expectation of privacy in a radio communication – e.g., due to encryption – however, the government may intentionally acquire the communication without a FISC order if the target is not a U.S. person and either the sender or any intended recipient is outside the United States.[126]

5. FISA's Current Definition of "Physical Search".

To understand the current definition of "electronic surveillance," it is also necessary to understand the current definition of "physical search." The definition of "physical search" functions in subchapter II of current FISA as the definition of "electronic surveillance" functions in subchapter I. It determines the FISC's jurisdiction,[127] the goal of a FISA application[128] and the subject-matter of an authorization order,[129] the scope of the President's power under FISA to act without FISC approval,[130] the scope of the limits on use of information derived from FISA,[131] the subject-matter of congressional reporting and oversight,[132] and the applicability of civil and criminal penalties for improper conduct.[133]

Fortunately, current FISA's definition of "physical search" is simpler than its definition of "electronic surveillance." Under 50 U.S.C § 1821(5), the term "physical search" means:

> [1] any physical intrusion within the United States[134] into premises or property (including examination of the interior of property by technical means) [2] that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, [3] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but [4] does not include (A) "electronic surveillance", as defined in section 1801(f) of this title, or (B) 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 1801(f) of this title.

Taking this definition one phrase at a time, a "physical intrusion ... into premises or property (including examination of the interior of property by technical means)" means physically entering a place protected by a reasonable expectation of privacy, or using technology to gain information about the interior of the place that would normally require a physical intrusion. Its meaning is illustrated by a 2001 Supreme Court decision, *Kyllo v. United States*.[135] In *Kyllo*, a federal agent in a car parked across the street from a private home used a "thermal imager" to scan and detect unusual heat patterns emanating from the home.[136] Based in part on those heat patterns, the agent "concluded that [Kyllo] was using halide lights to grow marijuana in his house, which indeed he was."[137]

The Supreme Court held that the thermal scan was a Fourth Amendment "search" requiring a warrant. It explained that until "well into the 20th century," Fourth Amendment jurisprudence "was tied to common-law trespass,"[138] which meant that while physical intrusion required legal justification, ordinary visual surveillance from a public place did not, because "the eye cannot by the laws of England be guilty of a trespass."[139] The issue for the Court in Kyllo was "how much technological enhancement of ordinary perception from such a [public] vantage point, if any, is too much."[140] The answer, according to the Court, was as follows: "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search – at least where (as here) the technology in question is not in general public use."[141] That appears to be the standard applicable to the phrase "examination of the interior of property by technical means" in FISA's definition of "physical search," although the matter is not clearly settled.

The second phrase in the definition – "seizure, reproduction, inspection, or alteration of information, material, or property" – also has a fairly settled meaning. The Supreme Court explained in *Kyllo* that the dictionary definition of "search" included to "look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief."[142] The Court has repeatedly held that a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[143] FISA's legislative history explains that the word "alteration" is

included in the definition to "ensure that the [FISC] is informed and approves of any planned physical alteration of property incidental to a search, e.g., the replacement of a lock so as to conceal the fact of the search."[144] The third phrase in the definition – "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – has the same meaning as its counterparts in the definition of "electronic surveillance," as discussed above.

The two exclusions in the current definition of "physical search" are important to the orderly functioning of FISA as a whole. The first exclusion – denoted [4](A) in the block quote above – simply means that the same conduct cannot be both electronic surveillance and a physical search; it must be one, or the other, or neither. The absence of a corresponding exclusion in the definition of "electronic surveillance" probably means that it yields only when it does not apply. Thus, where the same actions may be characterized as both electronic surveillance and as a physical search, they should be treated as surveillance. On that approach, use of the thermal imager in *Kyllo* should be "electronic surveillance" under Subsection (4),[145] because the imager is a "surveillance device" that was used "for monitoring to acquire information," even though the thermal scan could also be characterized as an "examination of the interior of property by technical means."

The second exclusion has the same function for certain foreign intelligence surveillance that is not "electronic surveillance" as defined by current FISA, and mirrors an exclusion in Title III.[146] As the 1978 legislative history of FISA explains, "the legislation does not deal with certain international signals intelligence activities currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."[147]

6. Application of FISA's Current Definitions.

As the foregoing discussion reveals, FISA's current definitions of "electronic surveillance" and "physical search" are very complex. Set out below are several hypothetical examples that may help illustrate the meaning of the definitions as applied to particular facts or scenarios.

a. Traditional Land-Line Telephone Calls.

It is "electronic surveillance" under current Subsection (1) if the government uses a surveillance device to acquire the contents of a cordless or corded land-line telephone call between a U.S. person in one state, Mr. *A*, and another person of any nationality in another state, Ms. *B* (it does not matter who called whom), without the consent of *A* or *B*, as part of surveillance targeting *A*. That is because a telephone call is either a "wire communication" (when intercepted from a wire) or a "radio communication" (when intercepted from the air); recording the call acquires its contents; the device used to record the call will be a "surveillance device"; *A* is the intentional target of the surveillance; *A* is a U.S. person; *A* is in the United States; there is a reasonable expectation of privacy in a telephone call;[148] and a Title III warrant would be required to conduct surveillance of the call for law enforcement purposes.[149]

The same is true if *B* is located abroad instead of in the United States, or if both *A* and *B* are in the same state (as long as they are using an interstate telephone company's facilities), regardless of where the surveillance occurs. As FISA's legislative history explains, Subsection (1) "protects U.S. persons who are located in the United States from being targeted in their domestic or international communications without a court order no matter where the surveillance is being carried out."[150]

If *A* (the target) is *not* a U.S. person, surveillance of the telephone call between *A* and *B* is not "electronic surveillance" under current Subsection (1). It is, however, "electronic surveillance" under current Subsection (2) if the contents of the call are acquired from a wire (not a radio signal), whether or not the government is targeting either *A* or *B* (or anyone else), as long as at least one of them is in the United States, the acquisition of contents occurs in the United States, and neither *A* nor *B* consents. Thus, again assuming that *A* is not a U.S. person, it is not "electronic surveillance" to acquire the contents of a call between *A* and *B* if both *A* and *B* are outside the United States, if the acquisition occurs outside the United States, or if one of them consents.[151]

If the contents of the call between *A* and *B* are intentionally acquired from a radio signal (not a wire), then the surveillance is "electronic surveillance" under current Subsection (3) if both *A* and *B* are located in the United States, regardless of where the surveillance occurs. Radio surveillance where *A* is not a U.S. person is not "electronic surveillance" if either *A* or *B* are outside the United States. Thus, if the government intercepts the radio portion of a cordless international call from a non-U.S. person in the United States, it probably is not electronic surveillance.[152]

b. Faxes.

Fax communications that transit conventional telephone lines should generally be indistinguishable from spoken telephone conversations under current FISA. Although a fax message is not an aural communication, like a telephone call, it is a "wire communication" under FISA while it is being carried on a wire, even though it would not be a "wire communication" under Title III.[153] A wireless fax machine would be treated like a cordless telephone, except that – because a fax is not aural and therefore may not be as easily intercepted – it would be even more likely than a cordless telephone call to generate a reasonable expectation of privacy.[154]

c. Mobile Telephone Calls.

Mobile telephones obviously raise geographical issues. When the government conducts surveillance of traditional land-line telephones (or fax machines), it knows where the telephone is located – that is the distinguishing feature of a land line. Thus, when the government monitors *A* talking (or faxing) on his home telephone, it can be reasonably confident that he is in fact at his home address. If *A* is a U.S. person, the government can therefore know, in advance, that the surveillance targeting him will be subject to current Subsection (1).

When *A* is using a mobile telephone, however, he may be virtually anywhere, including outside the United States.[155] When the government applies for a FISA order on A's mobile

telephone, it cannot know, in advance, whether or not he will use it to make calls from within the United States. Caution dictates obtaining a FISA order, of course, unless the government can be sure that *A* is in fact out of the country, but to the extent that *A* takes a temporary trip abroad, surveillance of calls made from his mobile phone may not be "electronic surveillance" under FISA.[156]

d. Microphones and Video.

If the government has a microphone concealed where *A* or *B* is located when making a private call (using any kind of telephone or other device), and the microphone acquires at least one side of the conversation, it is electronic surveillance under current Subsection (4) if the microphone is located in the United States. That is the case whether or not *A* and *B* are U.S. persons, and regardless of where *A* and *B* are located. The same holds true for microphone or video surveillance of *A* or *B* if they are engaged in an oral communication or even if they are not engaged in a conversation; "electronic surveillance" under current Subsection (4) applies to the acquisition of "information," not merely "communications."

e. E-Mail and Voice Mail Messages.

Electronic mail and voice mail messages raise difficult practical and legal issues under current FISA. The discussion begins with some background on how e-mail and voice mail function, and then considers the resulting legal implications under FISA.

i. Background on E-Mail and Voice Mail.

For purposes of the legal discussion that follows, here is a concrete (and somewhat oversimplified) description of how modern e-mail functions. The sender of an e-mail message writes the e-mail on his personal computer, which may be located virtually anywhere, using a software program like Microsoft Outlook or Eudora or AOL mail. He then hits the "send" button in that program, which transmits the e-mail message from his computer to his ISP. The e-mail is disintegrated into several discrete "packets" which are transmitted individually over the Internet – each packet may travel a different route from the others – until they converge at the recipient's ISP, where they are reintegrated into a coherent message that is stored on a server until the recipient logs in and reads the e-mail on his personal computer. Depending on whether the sender or recipient deletes the e-mail, and on their ISPs' own policies, the e-mail may remain in storage for some time after it has been read.[157]

Voice mail is similar in certain of those respects to e-mail: the caller telephones the recipient, and when no one answers, leaves a recorded message on the telephone company's electronic storage facilities. The recipient hears the recording when he dials in to those facilities to check his voice mail. Again, the voice mail is in storage with the telephone company at least until the recipient listens to it.

The foregoing descriptions reveal three important implications for the legal treatment of e-mail and voice mail under FISA. First, like mobile telephone calls, e-mails

and voice mails generate geographic issues: if *A* has an e-mail account with an ISP, he can access that account, and read his e-mail, from virtually anywhere in the world, including outside the United States. Again, therefore, the government cannot be sure that *A* will be in the United States when he sends or receives an e-mail. The same is true with respect to voice mail, which can also be accessed remotely.

Second, e-mail messages can be acquired after the fact from electronic storage in the sender's or recipient's e-mail accounts.[158] Unlike a plain old telephone service (POTS[159]) call, which involves a voice transmission over a dedicated circuit, e-mail messages are sent in the form of multiple packets that may travel over multiple electronic pathways from the sender to the recipient before being reassembled and stored for retrieval by the recipient. (This is the basic difference between a circuit-switched and packet-switched network.) Thus, unlike a telephone call, e-mail messages endure even after they have been sent, at a time when they are no longer "being carried" by a wire or radio wave.[160]

Third, e-mail and voice mail messages are communications entrusted to, and stored by, third parties, such as an ISP.[161] This raises a question about whether senders and recipients enjoy a reasonable expectation of privacy in the messages, and hence whether acquisition of them from an ISP or a telephone company is "electronic surveillance" or a "physical search" under FISA. Each of these three features – geography, storage, and the role of third parties – is considered in the discussion below.

ii. Acquisition of E-Mail (and Voice Mail) Under Current FISA.

The following paragraphs first address whether the acquisition of *stored* e-mail and voice mail is "electronic surveillance" (or a "physical search") as defined by FISA. They then address *transiting* e-mail.

Stored E-Mail. Stored e-mail and voice mail communications are neither "wire communications" nor "radio communications" under current FISA. As discussed above, the statute defines "wire communication" as a communication "while it is being carried by a wire."[162] Similarly, although the statute does not define "radio communication," every indication is that it includes communications only while they are being carried by radio wave. A stored communication – e-mail or voice mail – is not being carried by wire or radio wave,[163] and is therefore neither a wire nor a radio communication under current FISA. Subsections (1) – (3) of FISA's current definition of "electronic surveillance" apply only to "wire communications" and/or "radio communications."[164] Thus, acquisition of stored e-mail or voice mail is FISA "electronic surveillance," if at all, only under current Subsection (4).

For present purposes, current Subsection (4) requires two main elements: first, that there be the "installation or use" of a "surveillance device" in the United States "for monitoring to acquire information," other than from a wire or radio communication; and second, that the monitoring occur "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[165]

With respect to the first element of current Subsection (4), depending on the facts, acquisition of stored communications from an ISP or telephone company could involve a "surveillance device"; and if a surveillance device were involved, it would obviously be "installed or used."[166] It also seems likely that the acquisition of stored communications would involve "monitoring to acquire information." Obviously, when the government obtains copies of stored e-mails or voice mails it has "acquired information." Depending on the particulars of the acquisition, it would probably also involve "monitoring." There is a good argument that stored data as well as transiting data may be monitored: a grocery store clerk can monitor food items in the warehouse as well as on the shelves or in the check-out line. Reading an e-mail message stored on an ISP's server would be monitoring in the same way that reading a paper letter stored in a desk would be monitoring. There is also a good argument that monitoring need not be continuous: a doctor periodically monitors a patient's cholesterol as much as a lifeguard constantly monitors the water for swimmers in distress. Reading e-mails from a target's e-mail account once a day (or once a week) would be monitoring as much as reading them in real time as they arrive (although it is possible to imagine a court ruling otherwise). If a court determined that the first element were satisfied – i.e., that obtaining stored e-mail or voice mail involved the installation or use of a surveillance device for monitoring to acquire information – then the question would turn on the second element of the definition – i.e., whether this occurred in circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

On the other hand, if a court were to conclude that the acquisition of stored communications does *not* involve a "surveillance device" and/or "monitoring," and therefore is *not* "electronic surveillance," the court would then have to determine whether the acquisition satisfies FISA's definition of a "physical search." The current definition of a physical search also has two essential elements: first, it requires "any physical intrusion within the United States into premises or property ... that is intended to result in a seizure, reproduction, inspection or alteration of information, material, or property"; and second, like current Subsection (4) of the definition of "electronic surveillance," it requires that the intrusion occur "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[167] The first element of the definition of "physical search" is plainly satisfied: obtaining copies of e-mails from an ISP's server (in the U.S.) requires a "physical intrusion" – or its equivalent under *Kyllo* – into the ISP's premises, and it clearly results in a "reproduction" of "information." The same is true with respect to acquisition of voice mails from the U.S. premises of a telephone company.

Thus, the dispositive question is the same whether acquisition of stored e-mail and voicemail is analyzed as electronic surveillance (because it involves "monitoring" with a "surveillance device") or a physical search (because it does not involve monitoring with a surveillance device but does involve a physical "intrusion" and a "reproduction" of "information"). The question is whether the surveillance or search occurs "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[168] That question is addressed below.

In general, law enforcement officials must get a warrant to acquire stored e-mail and voice mail.[169] With a few exceptions, the Stored Communications Act provides that an ISP or

telephone company may not voluntarily disclose, and that law enforcement cannot compel disclosure of without a warrant, the contents of stored communications if those communications are less than six months old, at least until they are retrieved by the recipient. The Act provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service," and also that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."[170] An ISP or a telephone company is clearly a provider of "electronic communication service"[171] to the public, and stored e-mails and voice mails are clearly in "electronic storage" in an "electronic communications system," at least until they are retrieved by the subscriber.[172] Thus, in light of the Stored Communications Act, "a warrant would be required" to acquire stored e-mails or voice mails for law enforcement purposes, and the operative question under FISA is whether such acquisition occurs "under circumstances in which a party has a reasonable expectation of privacy."

There is an argument under existing case law that neither the sender nor the recipient of an e-mail (or voice mail) message enjoys a reasonable expectation of privacy in the message. In *Smith v. Maryland*,[173] the Supreme Court rejected the argument that the "installation and use" of a pen register violated a defendant's "'legitimate expectation of privacy' regarding the numbers he dialed on his phone." The Court relied in part on the fact that the defendant had voluntarily conveyed the numbers to the telephone company:

> Telephone users ... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[174]

The Court in *Smith* tied its narrow holding to the broader principle that there is no legitimate expectation of privacy in information voluntarily provided to third parties, as reflected in some of its prior decisions, including *United States v. Miller*,[175] which found no reasonable expectation of privacy in records about a defendant's financial transactions maintained by his bank.[176] The Court in *Smith* stated that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[177] It went on to explain:

> In *Miller*, for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to ... banks and exposed to their employees in the ordinary course of business." .... Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private. This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner

> voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[178]

Based on *Smith* and *Miller*, Congress in 1986 enacted the Stored Communications Act. As noted above, the Act provides statutory protection to stored communications, supplementing Title III's statutory protection for transiting communications, but it appears to be premised on the notion that such communications are not protected by the Fourth Amendment.[179] Indeed, certain provisions in the Act may be constitutional only if that is the case.[180]

If it were confronted with the constitutional question today, the Supreme Court might follow *Smith* and *Miller*, and reject any reasonable expectation of privacy for senders and recipients of e-mail and voice mail. However, the Court could find ways to distinguish both decisions if it wanted to.[181] Indeed, if it wanted to find a reasonable expectation of privacy in e-mail, the Court could rely on society's expectations derived from the Stored Communications Act itself,[182] or from the contractual arrangements between customers and their ISPs. One appellate court relied on an ISP's contractual arrangements and policies to find a reasonable expectation of privacy in e-mail.[183] Alternatively, Members of the Supreme Court more persuaded by common-law antecedents to the Fourth Amendment[184] could treat e-mail as the modern equivalent of postal mail, which has always been protected.[185] The issue is far from settled.[186]

Assuming for the moment that neither the sender nor the recipient of an e-mail or voice mail has a reasonable expectation of privacy in messages consigned to third parties, the third party itself – the ISP or telephone company – may have such an expectation that is relevant to FISA. Of course, the third party does not enjoy a reasonable expectation of privacy in the communication – e.g., in the e-mail's content. As noted above, however, the question under FISA is not confined to expectations of privacy in the content of acquired communications; it is whether the electronic surveillance or physical search conducted to acquire that content occurs under circumstances in which "a person" has a reasonable expectation of privacy. In most cases, the third party will retain a reasonable expectation of privacy in the place where the communications are stored and acquired.

Under Subsection (4) of the definition of "electronic surveillance," the precise question is whether "the installation or use" of the surveillance device occurs "under circumstances in which a person has a reasonable expectation of privacy."[187] Whether or not the "use" of the device to monitor a subscriber's e-mail would implicate an ISP's Fourth Amendment rights, certainly the "installation" of a device on its premises would do so. Thus, assuming that a "surveillance device" is installed and used for monitoring, acquisition of e-mails from an ISP is "electronic surveillance" under Subsection (4), either because the parties retain their expectation of privacy (despite *Smith* and *Miller*) in the content of the e-mail, or because the ISP retains its reasonable expectation of privacy in its e-mail servers where the surveillance device is installed.

A similar analysis applies under the definition of "physical search" if no surveillance device (or monitoring) is used. Apart from the "seizure, reproduction, inspection, or alteration"

that occurs once the government has arrived at the ISP or the telephone company, the "intrusion ... into premises or property" necessary to make the seizure would clearly implicate the third party's Fourth Amendment rights. Thus, acquisition of stored e-mail and voice mail (at least if unread and less than six months old) is either electronic surveillance or a physical search under FISA (it cannot be both).

Of course, if (based on *Smith* and *Miller*) the sender and recipient have no expectation of privacy in a stored communication, the third party could, as far as the Constitution is concerned, consent to its acquisition by the government and simply turn it over to the FBI upon request without the need for a warrant. However, as noted above, the Stored Communications Act generally forbids an ISP or telephone company from providing such consent.[188] Put another way, even with the third party's consent, a warrant would still be required for law enforcement purposes because of the Stored Communications Act. Thus, absent the consent of the sender or recipient, acquisition of stored e-mail or voice mail is "electronic surveillance" (or a "physical search") under FISA.[189]

Transiting E-Mail. As discussed above, e-mail differs from a telephone call in that it resides in electronic storage after being sent. The discussion thus far has analyzed acquisition of e-mail in storage. Acquisition of e-mail in real time, *before* the packets converge in the recipient's inbox, might or might not be "electronic surveillance," depending in the first instance on whether an ISP is a "common carrier" under FISA. There is no clear answer to this question in publicly-available materials, so it is necessary to address both possibilities.

If an ISP is not a common carrier, then e-mail transiting its wires or cables would not be a "wire communication" under FISA, and only current Subsection (4) would apply. Again, therefore, the question would reduce to whether a warrant is required to acquire transiting e-mail for law enforcement purposes. Although the Stored Communication Act would not govern – because transiting e-mail is not in storage – Title III itself requires a warrant to obtain transiting e-mail absent the consent of a party to the e-mail,[190] whether or not the party has a reasonable expectation of privacy under *Smith* and *Miller*.[191] Thus, absent the sender's or recipient's consent, using a surveillance device in the United States for monitoring to acquire transiting e-mail from an ISP that is not a "common carrier" under FISA would be "electronic surveillance."

Alternatively, if an ISP is a common carrier under FISA, then e-mail transiting its wires or cables would be a "wire communication," and current Subsection (2) – but not Subsection (4) – would apply.[192] Under Subsection (2), acquisition of the transiting e-mails would be "electronic surveillance" if either the sender or recipient were located in the United States, and neither party consented (or was a computer trespasser under Title III). The existence of a reasonable expectation of privacy would not matter. Absent the sender's or a recipient's consent, using a surveillance device in the United States to acquire transiting e-mail from an ISP that is a "common carrier" under FISA would be "electronic surveillance" if the sender or a recipient were in the United States.[193]

Finally, it is worth considering the results if, under any line of reasoning, acquisition of e-mail were held not to be "electronic surveillance" or a "physical search" under FISA. It would not leave the government free to acquire e-mail at will. On the contrary, it would mean that, as a

matter of statutory law,[194] the government generally could not acquire e-mail except by satisfying Title III, at least for domestic e-mails. That is because, as mentioned above, Title III generally prohibits interception of wire and electronic communications inside the United States absent consent and contains an exemption for conduct authorized by FISA.[195] Title III also contains an exemption for "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,"[196] but this exemption would not cover acquisition of domestic e-mail messages, and was enacted only to protect "certain international signals intelligence activities currently [as of 1978] engaged in by the National Security Agency."[197]

7. The Government's Proposal.

a. Overview.

It may be appropriate, before analyzing the government's proposal in detail, to focus on the motivations behind it. As far as I can tell, the government's proposal is animated by a desire not only to simplify the enormously complex definition of "electronic surveillance" in current FISA, but also to redress certain technological changes, and their legal consequences, that have occurred since the statute was enacted in 1978. In particular, the government has asserted publicly that FISA was not meant to reach most international (or at least transoceanic) communications because, in 1978, they were (generally) carried by radio rather than by wire.[198] As discussed above, under current FISA it is *not* "electronic surveillance" for the government to target a non-U.S. person by acquiring the contents of his international telephone calls while they are being transmitted as radio waves (rather than on a wire).[199] The government's argument, as I understand it, is that this exception was far more significant in 1978 than it is today, because – with the advent of fiber optic cables – international calls are now generally carried almost exclusively by wire, instead of by radio transmissions to and from satellites, leaving no opportunity for acquisition outside FISA's regulatory ambit.

I cannot comment further on this issue in this setting, but I do believe very strongly that it should inform any classified dialogue that ensues between Congress and the executive branch. Today's lawmakers obviously are not *bound* by the policy judgments of their predecessors in 1978, but I think they should make every effort to *understand* those judgments, and to determine how they have been affected by subsequent developments (technological or otherwise). These issues may be particularly important with respect to electronic mail, as discussed briefly below.

b. The Proposed Definition of "Electronic Surveillance".

Section 401(b) of the government's proposal would simplify, and narrow, FISA's definition of "electronic surveillance." In place of four subsections, the new definition would have two: essentially, it would cover (1) surveillance targeting individuals (U.S.

persons and non-U.S. persons alike) in the United States who enjoy Fourth Amendment rights, and (2) surveillance of purely domestic communications (i.e., communications solely within the United States). In place of six relevant factors, the new definition would have four:

(1) the type of information being acquired ("information" in general or a "communication" of any type);

(2) the type of acquisition (e.g., through the use of a surveillance device or the installation of such a device, or otherwise);

(3) the location of the targets and others (reasonably believed to be inside or outside the United States); and

(4) the existence (or not) of a reasonable expectation of privacy and the need (or not) for a warrant to engage in the surveillance under law-enforcement rules.

Presented in a chart, the new definition would look like this:

Statute	50 U.S.C. § 1801(f)(1)	50 U.S.C. § 1801(f)(2)
Type of information	Any information	Any communication
Type of Acquisition	Installation or use of an electronic, mechanical, or other surveillance device	Intentional acquisition of contents of any communication
Targets	Surveillance intentionally directed at a particular, known person	Communication is from a sender to one or more recipients
Location of Targets	That person is reasonably believed to be located within the United States	Sender and all intended recipients are reasonably believed to be in the U.S.
Reasonable Expectation of Privacy (REP) and Warrant Required for Law Enforcement (LE) Purposes	That person has a REP and warrant required for LE purposes	A person has a REP and warrant required for LE purposes

As I understand the government's proposal, most of the terms in its definition of "electronic surveillance" would be read according to (or in contrast with) their closest analogues in current FISA. I review both proposed subsections of the government's definition below.

i. Proposed Subsection (1).

The first clause of proposed Subsection (1) refers to the "installation or use of an electronic, mechanical, or other surveillance device for acquiring information." This is very close to language in current Subsection (4), which refers to "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information." The difference, of course, is that the government's proposal eliminates two restrictions – "monitoring" and "in the United States" – which should expand, rather than contract, the scope of the provision. In any event, the first clause of proposed Subsection (1) should be read by analogy to the corresponding language in current Subsection (4), which is discussed at length in the analysis of current FISA above.

The second clause in proposed Subsection (1) – "by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States" – has an analogue in current Subsection (1), which now applies to surveillance of a 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." Although the government has used slightly different words here, the concept of "intentionally directing surveillance" at a person is very close to the concept of "intentionally targeting" that person.[200] The "reasonably believed" modifier is probably intended to protect the government from liability in the event that it makes a (reasonable) error in determining the location of the target. As discussed above, electronic mail and mobile telephones raise geographical issues not present where landline telephones are concerned.

As discussed above, the reference to a "particular, known" person in current Subsection (1) is meant to cover watchlisting and similar activities, and – in my view – applies to any deliberate use of a surveillance device to monitor a specific communications channel where the but-for purpose of the surveillance is to acquire communications from a U.S. person in the U.S. As further discussed above, however, the remaining subsections of the current definition generally absorb any slack that arises from uncertainty about the meaning of this language.[201] For that reason, it would be of the utmost importance, before enacting the government's proposal, to ensure a common understanding of what it means to "intentionally direct[] surveillance at a *particular, known* person." The precise question is whether the government believes that proposed Subsection (1) excludes wide-ranging or "driftnet" surveillance, on the theory that the target of such surveillance is *all* persons (or a group of persons, or persons in general), rather than any "particular, known" person. If the government takes that position, its proposal (if enacted) would mean that a surveillance program like Operation Shamrock would be unregulated by FISA.[202]

In all candor, I cannot believe the government will take that position. I suspect, rather, that proposed Subsection (1) is meant to cover any surveillance that is intentionally directed at *any* person or persons – particularly known or otherwise – who are reasonably believed to be located within the United States. If that is the case, it may be possible to dispel any uncertainty by changing the language of proposed Subsection (1) in exactly that

way. In any event, to repeat, the issue should be resolved authoritatively so that no question remains for the future.

The third and final phrase in proposed Subsection (1) – "under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – differs from its closest analogue in current FISA because of its reference to "that person" rather than "a person." As discussed above, current Subsections (1), (3), and (4) apply when "a person" has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;[203] as a result, the reasonable expectation of privacy does not depend on the status of the particular individual whose privacy is being invaded by the surveillance.[204]

By referring to "that person," however, proposed Subsection (1) apparently would apply only when there is a reasonable expectation of privacy in the "particular, known" person at whom the surveillance is directed. Depending on the Fourth Amendment rights of non-U.S. persons in the United States, as discussed with respect to current FISA above, the government's proposal might not regulate surveillance of international communications targeting (certain) non-U.S. persons in the United States. Similarly, it might not regulate microphone or video surveillance of such persons, as long as the surveillance is not intentionally directed at their "communications" rather than other activities. That is because proposed Subsection (1) would not apply to the extent that non-U.S. persons do not enjoy Fourth Amendment rights, and proposed Subsection (2) – which follows the traditional approach in referring to "a person" – applies only to intentional surveillance of purely domestic communications, not to international communications, and not to any non-communicative conduct.[205]

This too strikes me as an issue that should be resolved firmly before enacting (or in the text of) any legislation. I note that here, too, any uncertainty would be eliminated if proposed Subsection (1) were changed to refer to *any* person or persons who are reasonably believed to be located in the United States, under circumstances in which *a* person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

ii. Proposed Subsection (2).

The first clause of proposed Subsection (2) refers to "the intentional acquisition of the contents of any communication." This is drawn from current Subsection (3), which applies to "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication." The reference to "intentional" acquisition, I think, is meant to exclude accidental, but inevitable, overcollection. If anything, I believe, such accidental overcollection is more of a problem today than it was in 1978, because of the proliferation of communications and communications technologies. One important change, of course, is that Section 401(e) of the government's proposal narrows the definition of "contents" to exclude routing and addressing information. As amended, contents would include only the "substance, purport, or meaning" of the communication, as is currently the case under Title III.

This is an interesting issue, but not one that I have had time to address at any length in these comments.

The second clause of proposed Subsection (2) – "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – is identical to the language in current FISA, and would be given the same meaning.

The third and final clause of proposed Subsection (2) restricts the provision to situations in which "the sender and all intended recipients are reasonably believe to be located within the United States." This obviously excludes any international communications – or any communications reasonably believed to be international.

c. Application of the Proposed Definition.

The government's proposed definition of "electronic surveillance," although simpler than current law, is still complex. Set out below are several hypothetical examples that may help illustrate the meaning of the definition as applied to particular facts or scenarios.

i. Traditional Land-Line Telephone Calls.

It is "electronic surveillance" under proposed Subsection (2) if the government intentionally acquires the contents of any telephone communication – mobile, cordless, or landline – between a person of any nationality reasonably believed to be in one state, Mr. *A*, and another person of any nationality reasonably believed to be in the same or another state, Ms. *B* (it does not matter who called whom). That is because proposed Subsection (2) applies to the intentional acquisition of the contents of "any" domestic communication in which there is a reasonable expectation of privacy and a warrant would be required for surveillance for law enforcement purposes. Subsection (1) also would apply to such surveillance, if the surveillance is effected using a device, and if the target of the surveillance – *A* or *B* – has a reasonable expectation of privacy (e.g., because of status as a U.S. person).

If *B* is located abroad instead of in the United States, then proposed Subsection (2) does not apply. However, if *A* is the target, and has a reasonable expectation of privacy, and if the surveillance is effected by a device, then the surveillance would be "electronic surveillance" under proposed Subsection (1). If both *A* and *B* are abroad, surveillance of their call would not be "electronic surveillance," as is the case under current law.

As noted above, there may be some uncertainty about "driftnet" surveillance of international calls, which would not be covered under proposed Subsection (2), to the extent that such surveillance is not considered to be intentionally directed at a "particular, known" U.S. person, within the meaning of proposed Subsection (1).

ii. Faxes.

Fax communications that transit conventional telephone lines should generally be indistinguishable from spoken telephone conversations under the government's proposal.

Although a fax message is not an aural communication, like a telephone call, it is a "communication" under the government's proposal.

iii. Mobile Telephone Calls.

Mobile telephones obviously raise geographical issues. When the government conducts surveillance of traditional land-line telephones (or fax machines), it knows where the telephone is located – that is the distinguishing feature of a land line. Thus, when the government monitors *A* talking (or faxing) on his home telephone, it can be reasonably confident that he is in fact at his home address. In such a case, the government can therefore know, in advance, that the surveillance targeting him will be subject to proposed Subsection (1) if that home address is in the United States (at least to the extent that *A* has Fourth Amendment rights).

When *A* is using a mobile telephone, however, he may be virtually anywhere, including outside the United States. When the government applies for a FISA order on *A*'s mobile telephone, it cannot know, in advance, whether or not he will use it to make calls from within the United States. Caution dictates obtaining a FISA order, of course, unless the government can be sure that *A* is in fact out of the country, but to the extent that *A* takes a temporary trip abroad, surveillance of calls made from his mobile phone would not be "electronic surveillance" under the government's proposal.

iv. Microphones and Video.

If the government has a microphone concealed where *A* or *B* is located when making a private call (using any kind of telephone or other device), and the microphone acquires at least one side of the conversation, it is electronic surveillance under proposed Subsection (1) if the target – *A* or *B* – is located in the United States and enjoys a reasonable expectation of privacy. That is the case whether or not *A* and *B* are U.S. persons, and regardless of where the microphone is located. The same holds true for microphone or video surveillance of *A* or *B* if they are engaged in an oral communication or even if they are not engaged in a conversation; "electronic surveillance" under proposed Subsection (1) applies to the acquisition of "information," not merely "communications."

v. E-Mail and Voice Mail Messages.

Electronic mail and voice mail messages raise difficult practical and legal issues under the government's proposal, but the issues may be different, and perhaps less amenable to public discussion, than those raised under current FISA. The discussion below assumes familiarity with the explanation of e-mail in the analysis of current FISA above.

Although stored e-mail is not a "wire communication" or a "radio communication" under current FISA, it probably is a "communication," and transiting e-mail certainly is a "communication." Thus, surveillance of the contents of such e-mail satisfies the first clause of proposed Subsection (2). The next clause of the proposal concerns whether "a person" has a reasonable expectation of privacy in the e-mail message, and whether a warrant

would be required to acquire the contents of the e-mail for law enforcement purposes.[206] For now, it is appropriate to assume, based on the earlier discussion of the same issue under current FISA, that this clause is satisfied. That leaves the third and final clause of Subsection (2), which turns on whether the "sender and all intended recipients" of the e-mail are reasonably believed to be located in the United States. This raises technically complex – and somewhat metaphysical – questions that I am not at liberty to discuss here.[207] I recommend that Congress take up the issue with the executive branch in detail in an appropriate closed session. The same applies with respect to analysis under proposed Subsection (1), at least if the target of the surveillance is located in the United States.

8. Intersection With Title III.

By narrowing the definition of "electronic surveillance" in FISA, the government's proposal may raise issues under Title III, the criminal wiretapping statute. Title III sets out a broad rule against electronic surveillance and the use or disclosure of information obtained from electronic surveillance "[e]xcept as otherwise specifically provided in this chapter."[208] In particular, Title III generally prescribes criminal penalties for anyone who (1) "intentionally *intercepts*, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication";[209] (2) "intentionally *discloses*, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection";[210] or (3) "intentionally *uses*, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection."[211]

Title III's definitions[212] mean that its general prohibition on the interception of wire, oral, and electronic communications includes almost all of what FISA currently defines as "electronic surveillance"[213] conducted inside the United States. Correspondingly, Title III's general prohibition on use or disclosure of information obtained from such interceptions therefore includes uses or disclosures authorized under FISA and FISA minimization procedures. Thus, the issue arises whether Title III forbids what FISA expressly permits.

Fortunately, under current law, a conflict between the statutes is averted because Title III explicitly authorizes electronic surveillance under FISA:

> Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.[214]

Thus, Title III's general prohibition of the interception of wire, oral, or electronic communications, and its derivative prohibitions of the use or disclosure of information obtained from unauthorized interceptions, do not apply to "electronic surveillance" authorized by the

current version of FISA, or to the use or disclosure of information obtained from such "electronic surveillance."

If Section 401(b) of the government's proposal were enacted, Title III's exception authorizing "electronic surveillance" as defined by FISA would be narrowed – because FISA's definition of "electronic surveillance" would be narrowed – and to that extent there might be a conflict between the two statutes. Some (if not most) of that conflict will be resolved by 18 U.S.C. § 2511(2)(f),[215] and by Section 402 of the government's proposal (discussed below, which authorizes conduct that is *not* "electronic surveillance" under FISA, and which applies "notwithstanding any other law"), but I would need a few more hours to work through all of the legal and operational possibilities to be sure. I assume the government already has done that, but it is an issue that should be very carefully considered.

Section 402

Section 402 of the government's proposal would significantly expand the Attorney General's power to authorize electronic surveillance of foreign powers without judicial review under 50 U.S.C. § 1802. This would be another very significant change in the law.

1. Background on Current 50 U.S.C. § 1802.

Under the current version of 50 U.S.C. § 1802, the government may conduct electronic surveillance of certain foreign powers without judicial approval. The statute provides that "[n]otwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order ... to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath" three essential requirements.[216]

The first requirement is exclusivity: the electronic surveillance must be directed solely at communications channels used exclusively by official foreign powers, or at acquisition of technical intelligence from property "openly and exclusively controlled" by official foreign powers, and the physical search must also be directed solely at such property or at property "used exclusively" by official foreign powers. The second requirement is that there be "no substantial likelihood" that the search or surveillance will infringe on a U.S. person's privacy interests. Third and finally, the surveillance or search must be conducted in accord with minimization procedures that are reported to Congress. The Attorney General's certification of these three elements must be transmitted to the FISC for safekeeping, although the FISC does not review the certification.[217] The Attorney General may also direct a specified communications common carrier, landlord, or other specified person to assist in implementing the surveillance or search and to maintain records pertaining to the surveillance or search under proper security procedures.[218]

Before discussing each of the three requirements in detail, it is worth noting that Sections 1802 and 1822 reflect a political compromise, crafted in 1978, between those who believed that "a warrant should be required across-the-board" for all electronic surveillance under FISA, and those who "felt that a judge should never be involved."[219] In

the end, the "consensus" was that "a judicial warrant should be required whenever the Fourth Amendment rights of Americans might be involved."[220] Based on testimony "taken in closed session, [the House Intelligence] committee determined that there was a class of surveillances, otherwise within the scope of the bill, where there was little or no likelihood that Americans' Fourth Amendment rights would be involved in any way. The committee also determined that this class of surveillances included some of the most sensitive surveillances which this Government conducts in the United States."[221] The result was Section 1802, and later its counterpart for physical searches, Section 1822.

a. Exclusive Use or Control by an Official Foreign Power.

Under current Section 1802, the electronic surveillance must be "solely directed at" acquisition of "the contents of communications transmitted by means of communications used exclusively between or among foreign powers,"[222] or acquisition of "technical intelligence other than the spoken communications of individuals, from property under the open and exclusive control of a foreign power."[223] (Under Section 1822, the physical search must be "solely directed at" the "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[224])

The "foreign powers" in question under both provisions must be "official" foreign powers as defined in 50 U.S.C. §§ 1801(a)(1)-(3).[225] That is, they must be "a foreign government or any component" of a foreign government; a "faction" of a foreign nation or nations "not substantially composed of U.S. persons," such as the PLO;[226] or an entity "openly acknowledged" by a foreign government or governments to be "directed and controlled" by those government or governments, such as a state airline or OPEC.[227] Sections 1802 and 1822 do not extend to other foreign powers, such as international terrorist groups.

Sections 1802 and 1822 apply to property or premises under the "open and exclusive control" of foreign powers (and Section 1822 also applies to physical searches of property "used exclusively by" foreign powers).[228] This would cover a foreign government's embassy or diplomatic mission, or other facilities owned by an official foreign power from which outsiders may be excluded.[229] Both provisions currently authorize the surveillance or search "notwithstanding any other law," and the statute's 1978 legislative history explains that the phrase was used in FISA to make clear that "the activities authorized in the bill are not prohibited by the Vienna Convention on Diplomatic Relations."[230] The Vienna Convention establishes protocols under which "sending States" establish diplomatic missions in "receiving States," provides that the "premises of the mission shall be inviolable," and in particular provides that the "agents of the receiving State may not enter them, except with the consent of the head of the mission."[231] Sections 1802 and 1822 seem clearly to contemplate violations of the Vienna Convention.[232] In 2003, the Department of Justice wrote in a draft summary of proposed legislation that "[i]n essence, § 1802 authorizes the surveillance of communications between foreign governments, and between a foreign government and its embassy."[233]

Section 1802 also applies to acquisition of "technical intelligence, other than spoken communications of individuals," acquired from such exclusively controlled property. The term

"technical intelligence" is not defined in the statute, and the legislative history warns that it "cannot elaborate on the activities covered" by this provision.[234] Nor can I.

b. No Substantial Likelihood of Surveilling or Searching U.S. Persons.

In addition to the first requirement, concerning exclusivity, both Section 1802 and Section 1822 today contain a second requirement, in that they apply only where there is "no substantial likelihood" that the electronic surveillance will acquire the contents of any "communication to which a U.S. person is a party" or that the search will involve the "premises, information, material, or property" of a U.S. person.[235] This second requirement directs the government to predict the likelihood of infringing on U.S. person privacy interests, with the Attorney General certifying the prediction "in writing under oath."[236]

To some degree, the second requirement duplicates the first. If a communications system is indeed used exclusively by official foreign powers, then the odds of acquiring communications to or from a U.S. person seem remote. But there may be cases in which the second requirement operates independently. For example, a "foreign power" as used in Sections 1802 and 1822 includes a "faction" of a foreign nation such as the PLO.[237] Such a faction may include some U.S. persons, as long as they do not make up a "substantial" portion of the faction.[238] If such a faction, partially but not substantially composed of U.S. persons, had open and exclusive control of premises in the United States, the first requirement of Sections 1802 and 1822 would be satisfied, but the second requirement might not be.

c. Minimization.

A surveillance or search under current Sections 1802 and 1822 must be conducted in accordance with "minimization procedures" that meet the statutory requirements and that are reported in advance, or promptly after the fact where necessary, to the House and Senate Intelligence Committees.[239] The Attorney General must also assess compliance with the minimization procedures and report on the assessment as part of the semi-annual report to the Intelligence Committees.[240]

Minimization procedures must address the possibility that, despite the Attorney General's expectations and certification under oath, a surveillance or search may acquire or involve a U.S. person's communications or property. If that occurs, the government must obtain an approval order from the FISC. The statute currently provides that such information may not be retained or used "for any purpose" for longer than 72 hours unless "a court order" approving the surveillance or search "is obtained" or unless the Attorney General determines that "the information indicates a threat of death or serious bodily harm to any person."[241] As a technical matter, this means that the government must file its application, and the FISC must issue its order, within 72 hours after the U.S. person information is acquired. Even if the government timely files the application, if the FISC does not rule and issue its order quickly, the information would need to be destroyed (absent a threat of death or serious bodily harm).

2. The Government's Proposal.

Under the government's proposal, Section 1802 would be expanded significantly. It would apply to surveillance "directed at," rather than "solely directed at," an official foreign power, and to surveillance of all communications of such a foreign power rather than communications made on facilities used "exclusively between or among foreign powers." In other words, the provision apparently would apply to *any* communications facility used by, or about to be used by, a foreign power.[242] Correspondingly, the government's proposal would eliminate the requirement that there be "no substantial likelihood" of acquiring a U.S. person's communications. If surveillance is to include facilities used by U.S. persons, then the Attorney General obviously cannot certify that U.S. persons will not be surveilled. And, of course, Section 401(d) of the government's proposal deletes current 50 U.S.C. § 1801(h)(4), the minimization provision that effectively requires sequestration of U.S. persons' communications which are (despite expectations) acquired under current 50 U.S.C. § 1802.

Section 402 of the government's proposal would also enact new 50 U.S.C. § 1802A, which applies to the acquisition of foreign intelligence information using methods that are *not* "electronic surveillance" under certain circumstances. The circumstances would be (1) that the surveillance is to acquire foreign intelligence information "concerning persons reasonably believed to be outside the United States"; (2) that the information be obtained from a communications provider or other third party; (3) that a significant purpose of the surveillance be to obtain foreign intelligence information; and (4) that proper minimization procedures be followed. Where these conditions are met, Section 402 of the government's proposal would allow the Attorney General to authorize surveillance (and other collection) activity without a court order for one-year periods.

This provision, which applies only to conduct that is *not* "electronic surveillance" as defined by FISA, obviously takes on added significance when paired with the narrowing of that definition in Section 401(b) of the government's proposal. As discussed above, Section 401(b) might exclude from "electronic surveillance" certain kinds of non-targeted "driftnet" surveillance of international communications. To the extent that is the case, those kinds of surveillance would be within the scope of 50 U.S.C. § 1802A as proposed by the government. Indeed, proposed 50 U.S.C. § 1802A(b), which provides that the surveillance need not be confined to a particular communications facility, seems to confirm the breadth of the provision. The provision seems designed for collection wholesale – it seems to signal this intention by providing explicitly that it applies *only* to acquisition from or with the assistance of communications providers. It would be very important to determine how proposed Section 1802A would affect existing or contemplated surveillance activity like the (judicial or non-judicial versions of the) Terrorist Surveillance Program (TSP).

Proposed Section 1802A applies only to the acquisition of foreign intelligence information "concerning" persons reasonably believed to be abroad, and only when there is a "significant purpose" to obtain foreign intelligence information. This does not mean that it requires the surveillance *targets* to be abroad, but only that the information obtained

concern someone (reasonably believed to be) abroad. Moreover, it may be that acquisition of such information need only be a significant purpose of the surveillance, arguably leaving room for the primary purpose to be acquisition of other types of foreign intelligence information.[243]

Finally, it is also worth noting that this provision could be read as a Congressional endorsement of one-year periods of surveillance for U.S. persons under Section 2.5 of Executive Order 12333.[244] The statute would not resolve the "reasonableness" of such surveillance, of course, but it would probably have some influence on a judicial determination of that Fourth Amendment question.

I have not examined closely the elements of proposed 50 U.S.C. § 1802B, which would allow the Attorney General to compel assistance from a third party provider. This handmaiden provision probably should rise or fall with proposed 50 U.S.C. § 1802 and 1802A, and any technical errors should be relatively easy to repair. (It may be the case that, even if 50 U.S.C. § 1802 remains unchanged, the government needs some sort of compulsory provision directed at communications providers; if that is the case then proposed Section 1802B might still be useful.)

Nor have I examined closely proposed 50 U.S.C. § 1802C, which appears to import FISA's suppression and discovery provisions to surveillance conducted under proposed 50 U.S.C. § 1802A. Again, this provision rises or falls with 50 U.S.C. § 1802A, and should be relatively straightforward as a technical matter.

Section 403

This provision makes sense to me. Adding "at least" before the reference to seven circuits is appropriate now that the FISC consists of eleven (rather than seven) judges. The Chief Justice, who appoints judges to the FISC, has (correctly) interpreted the statute that way since the USA PATRIOT Act, but it is wise to make the matter explicit. Nor do I see any problem with moving what is now 50 U.S.C. § 1802(b) into 50 U.S.C. § 1803. I would consider changing "the purpose" to "a significant purpose" in the moving language, but I do not consider it essential. I note the absence of the requirement that the President have, by written designation, empowered the Attorney General to approve applications to the FISC, but if such a provision raises separation-of-powers concerns, I have no strong objection to its omission.

Section 404

Section 404 of the government's proposal would reduce the required elements of an ordinary FISA application for electronic surveillance. It may therefore be helpful to begin with a description of the current requirements of such an application.

1. Current Law Governing FISA Applications.

Under current law, applications for court orders authorizing electronic surveillance or physical searches (or both[245]) under FISA are made to the FISC under oath by a federal officer with the approval of the Attorney General, the Acting Attorney General, the Deputy Attorney

General, or – if designated by the Attorney General – the Assistant Attorney General for National Security.[246] Typically, such an application includes statements made by an attorney in the Office of Intelligence Policy and Review (OIPR), a component of the Department of Justice[247] that represents the federal government before the FISC, as well as an affidavit (referred to in the government as a "declaration") from an investigating agency such as the FBI.[248]

a. Contents of Application.

To meet the statutory requirements in current FISA, the application must provide the identity of the applicant[249] and include information concerning the following (items marked with an asterisk, rather than a bullet point, would change if Section 404 of the government's proposal were enacted):

- *Who is being searched or surveilled.* The application must include the "identity, if known, or a description of the [specific] target."[250]

- *Why the target lawfully may be searched or surveilled.* The application must include a statement of facts that is "relied upon by the applicant to justify his belief,"[251] and used by the FISC to determine probable cause, that the target of the surveillance or search is a "foreign power" or an "agent of a foreign power."[252]

- *A nexus between the target and the location of the search or surveillance.* In electronic surveillance cases, the application must include a statement to establish 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."[253] In physical search cases, it must include a statement to establish that "the premises or property to be searched contains foreign intelligence information,"[254] and that it "is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power."[255]

- *A description of what is to be searched or surveilled.* In electronic surveillance cases, the application must include a description of "the type of communications or activities to be subjected to the [electronic] surveillance."[256] In physical search cases, it must include a "detailed description of the premises or property to be searched and of the information to be seized, reproduced, or altered."[257]

* *The nature of the information sought by the search or surveillance.*[258]

- *Limits on the search or surveillance.* The application must contain a statement of "proposed minimization procedures."[259]

* *An explanation of how the search or surveillance will be carried out.* In electronic surveillance cases, the application must include a statement of "the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance."[260] In physical search cases, it must include a description of "the manner in which the physical search is to be conducted."[261] In addition, in physical

search cases only, the government must file a return with the FISC upon completion of the search that reports its "circumstances and results."[262]

* *An account of any prior FISA applications*. The application must include a statement "concerning all previous applications" involving any of the persons, facilities, places, premises, or property specified in the current application, and the action taken on each previous application.[263]

In addition, in electronic surveillance cases only, the application must also include statements concerning the following two additional matters:

- "[T]he period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter."[264]

* "[W]henever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device."[265]

b. Mechanics and Accuracy of Application.

As the FBI observed in the spring of 2001, "[i]n recent years, applications for electronic surveillance or physical search authority submitted to the [FISC] have evolved into increasingly complex documents. The heart of these applications is the declaration, signed by a supervisory special agent at FBIHQ [FBI Headquarters in Washington, D.C.], which sets out the factual basis supporting probable cause for the requested authority and which conveys to the FISC any other facts relevant to the Court's findings."[266] This observation highlights an important distinction between FISA applications and applications for search warrants and Title III orders used in conventional criminal investigations. Unlike an ordinary search warrant or Title III order, which can be issued by a local federal judge in any judicial district, FISA orders are issued only by the FISC, a court that sits in Washington, D.C. In part because the FISC's practice is often to have the declarant appear in person, and in part because of the coordinating role played by FBIHQ in NSIs, the FISA declaration is typically signed by a headquarters agent.[267]

This creates a potential problem: although the FISA declarant resides in Washington, D.C., the facts in the declaration may nonetheless pertain to NSIs being conducted in any FBI field office, from Seattle to Miami. As the FBI has explained, "[t]he information currently required for a FISA declaration, in many cases, is extensive, and often includes descriptions of operations, criminal investigations, or prosecutions well outside the personal, or even programmatic, knowledge of the Headquarters supervisor who will serve as the declarant."[268] Procedures adopted by the FBI in April 2001 (and later declassified) are designed to "ensure accuracy" in FISA declarations concerning the facts supporting probable cause, the nature of

related criminal matters; and the "existence and nature of any prior or ongoing asset relationship between the subject [i.e., the FISA target] and the FBI."[269]

These so-called "Woods Procedures," named after the capable FBI attorney who was their principal drafter, require FBI agents in the field and at headquarters to (1) search electronic databases and files for references to the FISA target, document the results of those searches, and complete a "FISA Verification Form"; (2) review, edit, and approve the declaration for factual accuracy; and (3) collect all relevant documentation of the required reviews. In cases where multiple field offices may be involved, each field office must review the application. In cases where criminal investigations are being conducted, the criminal agents must also review relevant portions of the declaration.[270] The procedures are elaborate and exacting, but they appear to have worked well.[271]

c. Certification.

To obtain approval for electronic surveillance or physical search under current law, the government must also submit to the FISC a written certification from a high-ranking executive branch official.[272] The only certifying official specifically mentioned in FISA is the "Assistant to the President for National Security Affairs" – commonly referred to as the National Security Advisor.[273] Other persons may certify only if they are "an executive branch official ... designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate."[274] Typically, the Director of the FBI certifies FISA applications from the FBI,[275] and the Secretary or Deputy Secretary of Defense certifies applications from the NSA.[276] (As discussed below, Section 404 of the government's proposal would change the permissible rank of the certifying official to include any federal official.)

Under current law, the certification must do all of the following (items marked with an asterisk, rather than a bullet point, would change if Section 404 of the government's proposal were enacted):

- **State that the certifying official "deems" the information sought to be "foreign intelligence information."[277]**
- **State that a "significant purpose" of the electronic surveillance or physical search is to obtain foreign intelligence information.[278]**
- **State that such information "cannot reasonably be obtained by normal investigative techniques."[279]**
- * **Designate "the type of foreign intelligence information being sought according to the categories described in" the definition of "foreign intelligence information."[280]**

Under current law, the certification must also include "a statement of the basis" for the latter two elements – that the information sought is the type of foreign intelligence

designated and that it cannot reasonably be obtained by normal investigative means.[281] (This too would change under the government's proposal.) The certification is effectively an affidavit,[282] and the 1978 House report on FISA explains that its purpose is to

> **insure that a high-level official with responsibility in the area of national security will review and explain the executive branch determination that the information sought is in fact foreign intelligence information. The requirement that this judgment be explained is to insure that those making certifications consider carefully the cases before them and avoid the temptation simply to sign off on certifications that consist largely of boilerplate language. The committee does not intend that the explanations be vague generalizations or standardized assertions.... The designated official must similarly explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important in those cases when U.S. citizens or resident aliens are the target of the surveillance.[283]**

Where the FISC is dissatisfied with the certification, it can require additional certifications.[284]

d. Attorney General Approval.

The final element in a FISA submission seeking an electronic surveillance or physical search order from the FISC is the citation of the Attorney General's authority, conferred by the President, to file FISA applications,[285] and the Attorney General's written approval of the particular FISA application being filed "based upon his finding that it satisfies" the statutory requirements.[286] The 1978 legislative history of FISA explains the purpose of this approval requirement:

> Each application must be approved by the Attorney General, who may grant such approval if he finds that the appropriate procedures have been followed. The Attorney General's written approval must indicate his belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause that the target is a foreign power or an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed are being used, or about to be used, by a foreign power or an agent of a foreign power, and that all other statutory criteria have been met. In addition, the Attorney General must personally be satisfied that the certification has been made pursuant to statutory requirements.[287]

This is a heavy responsibility, but the Attorney General need not face it alone. If necessary, the Attorney General may "require any other affidavit or certification from any other officer in connection with the [FISA] application."[288]

On the other side of the balance, in certain cases, another high-ranking executive branch official may force the Attorney General's personal involvement in reviewing a FISA application.

Under two provisions of the current statute, "the Attorney General shall personally review" a FISA application for electronic surveillance or physical search of certain FISA targets upon written request from the Director of the FBI, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence (DNI).[289] This obligation is not delegable by the Attorney General (or any of the other officials mentioned) except "when disabled or otherwise unavailable."[290] If the Attorney General does not approve the application, he or she must give written notice to the requesting official and explain the changes needed to secure approval.[291] The requesting official must then modify the application if he or she believes it is appropriate to do so.[292] As discussed below, the government's proposal would add the Director of the CIA to the list of officials covered by this provision.

In physical search cases involving "the residence of a United States person,"[293] the Attorney General must also "state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information."[294]

As enacted in 1978, FISA defined "Attorney General" to include the Attorney General, the Acting Attorney General, or the Deputy Attorney General. In 2006, the statute was amended to provide that the "Attorney General" also includes the Assistant Attorney General for the National Security Division, if designated by the Attorney General.[295]

2. <u>The Government's Proposal</u>.

The most significant part of Section 404 of the government's proposal would change the permissible status of the certifying official. It would allow the President to designate *any* executive branch official as the certifier. Presumably, this is designed to let the President designate one or more NSA shift supervisors or other mid-level managers. While I can see the need to expand the roster of certifying officials, under current law the President is free to do so by naming any Senate-confirmed official. The burden of persuasion that the government needs a broader and lower-ranking pool of candidates should be relatively high, in my opinion, because the inevitable risk of such a move is to denigrate the significance of the certification.

Section 404 also would eliminate the requirement that "whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device."[296] I can understand the government's aversion to this provision, but I would not jettison it lightly, at least without some explanation.

Other changes in Section 404 of the government's proposal are less significant. Section 404 would eliminate the requirement, now totally boilerplate, that every FISA application recite the authority conferred on the Attorney General by the President to make the application.[297] This is similar to the change in Section 403 of the government's proposal discussed above; it provokes no strong reaction in me. The various changes from "detailed statement" to "summary statement" may not be very significant in operational effect, because the FISC will still be able to demand the level of detail that it finds appropriate.

Section 405

As time was running out on this project, I quickly scanned Section 405 of the government's proposal. As far as I can tell, apart from making changes corresponding to Section 404, it does the following. **First, it increases the duration of certain surveillance of non-U.S. persons who are agents of foreign powers, and (unless I am misreading) it may allow one-year renewal periods even for U.S. persons. It also increases the duration of emergency surveillance to one week, and – to my surprise – seems to suggest that the Attorney General must personally notify the FISC when he authorizes such surveillance (because it seems to delete any reference to his "designee" – perhaps general delegation principles are thought to make that superfluous). It appears to eliminate any second-guessing of the Attorney General's use of emergency surveillance, removing the word "reasonably" before "determines" in current 50 U.S.C. § 1805(f), and adding "determines that" before "the factual basis exists" in current 50 U.S.C. § 1805(f)(2).** And it expands the circumstances in which the "take" from unratified emergency surveillance may be used.

Section 406

Section 406 of the government's proposal may take on added significance with the amendments to the definition of "electronic surveillance" contained in Section 401(b) of the government's proposal. I have no objection to the government's preservation of its privileges in the paragraph (2) of the proposal.

Section 407

Section 407 of the government's proposal addresses weapons of mass destruction. It would expand the definition of "foreign power" to include a group engaged in the "international proliferation of weapons of mass destruction," expand the definition of "agent of a foreign power" to include a non-U.S. person who engages in such proliferation, and expand the definition of "foreign intelligence information" to include information necessary or relevant to the ability of the United States to protect against such proliferation. Conceptually, this provision may make sense – i.e., there may be examples, available for discussion in a classified setting, of cases where weapons of mass destruction, but *not* terrorism, are involved. **I am uncertain, however, about the breadth of the definition of "weapon of mass destruction"; for example, it seems to include even a very large caliber semiautomatic handgun.**[298]

Section 408

I have no comment on this provision.

Section 409

I assume (but have not checked) that this provision, which applies to physical searches, corresponds to the changes made in other provisions of the proposal that govern electronic surveillance. If so, most of my comments above would apply. It would be important to ensure

that the government has worked through the relationship between the definition of "electronic surveillance" and the definition of "physical search."

Section 410

If emergency electronic surveillance is to endure for a week, under Section 405 of the government's proposal, then it makes sense to apply the same standard to pen/trap surveillance.

Section 411

I have no comment on this provision.

Section 412

I did not read this provision, taking seriously the title's assertion that it contains only "technical and conforming amendments."

Section 413

I have no comment on this effective date provision of the statute.

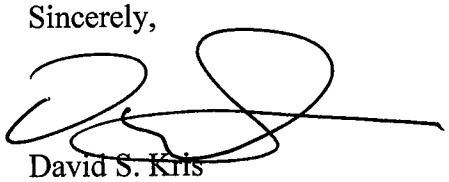
Section 414

I have no comment on this severability provision of the statute.

* * *

Thank you very much for the opportunity to comment on this interesting proposal.

Sincerely,



David S. Kris

P.S. The notes begin on the next page.

NOTES

[1] I was first contacted about providing comments on the afternoon of Wednesday, April 25. As a former government employee, I submitted an initial draft of this letter to the Department of Justice (DOJ) on Friday morning, April 27, and subsequent drafts over the course of the weekend, for prepublication review under 28 C.F.R. § 17.18. I am grateful to DOJ for its extremely rapid review. This letter reflects only my own views, not those of any other person or entity, including DOJ. Some of the material in this letter is derived from a treatise that I co-authored with Doug Wilson, *National Security Investigations and Prosecutions*, which is forthcoming from Thomson-West publishing.

[2] H.R. Rep. No. 95-1283, Part I, at 68 (1978) [hereinafter FISA House Report].

[3] The electronic surveillance provisions of FISA, enacted in 1978, refer to "his belief." 50 U.S.C. § 1804(a)(4). The physical search provisions, enacted in 1994, are gender neutral and refer to "the applicant's belief." 50 U.S.C. § 1823(a)(4).

[4] 50 U.S.C. § 1804(a)(4)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(4)(A) (physical search). Correspondingly, to approve the FISA application, the FISC must find probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3)(A) (electronic surveillance); 50 U.S.C. § 1824(a)(3)(A) (physical search).

[5] The certification provisions are at 50 U.S.C. § 1804(a)(7) (electronic surveillance) and 50 U.S.C. § 1823(a)(7) (physical search). The definition of "foreign intelligence information" is at 50 U.S.C. § 1801(e).

[6] 18 U.S.C. § 2510 et seq. For a more complete discussion of the FISA application process, see my comments on Section 404 of the government's proposal, below.

[7] See 50 U.S.C. § 1801(a) and (b).

[8] 50 U.S.C. § 1801(a)(4) ("a group engaged in international terrorism or activities in preparation therefor").

[9] See FISA House Report at 67 ("while it is expected that most entities would be targeted under the 'foreign power' standard (which cannot be applied to individuals), it is possible that entities could be targeted under certain of the 'agent of a foreign power' standards"). In *United States v. Rahman*, 861 F. Supp. 247, 251 (S.D.N.Y. 1994), one of the defendants claimed that only an "international organization" could be an agent of a foreign power. As the court pointed out, that claim flies in the face of the plain language of the statute, which refers to both "person[s]" and "members" of groups.

FISA actually contains two sets of definitions of the term "agent of a foreign power." The first set, in 50 U.S.C. § 1801(b)(1)(A)-(C), applies to "any person other than a United States person" and therefore does not extend to persons or entities that satisfy the definition of "United States person" in 50 U.S.C. § 1801(i). (A U.S. person includes a citizen of the United States and a lawful permanent resident alien – i.e., a person who has been issued Form I-551. See 8 C.F.R. § 264.1). This first set of definitions does not require the government to establish any criminal conduct by the putative agent of a foreign power. The second set of definitions, in 50 U.S.C. § 1801(b)(2)(A)-(E), applies to "any person," including a U.S. person. These definitions require a stronger showing that the target is acting on behalf of a foreign power, and some showing that his activities violate or may violate criminal law.

[10] This amendment was made by the Intelligence Reform and Preventing Terrorism Act of 2004, Pub. L. 109-177, 120 Stat. 192 (2004), and is now codified at 50 U.S.C. § 1801(b)(1)(C).

[11] See *In re Sealed Case*, 310 F.3d 717, 723 n.9 (FISCR 2002).

[12] 50 U.S.C. § 1801(e)(1).

[13] 50 U.S.C. § 1801(e)(2).

[14] FISA House Report at 47.

[15] *Id.*

[16] *Id.*

[17] FISA House Report at 48 (emphasis added); see also H.R. Rep. No. 98-738, at 17-18 (1984) [hereinafter FISA House Five Year Report] (allowing indexing and logging of acquired communications of U.S. persons if they "reasonably appear" to be foreign intelligence information"). Under the declassified version of the standard minimization procedures in effect as of 1984, information was to be retained if it "reasonably appear[ed]" to be foreign intelligence information. See *id.*

[18] See FISA House Report at 58 (when government is wiretapping a known spy, it is "'necessary' to acquire, retain, and disseminate information concerning all his contacts and acquaintances and his movements").

[19] The information normally will be "concerning" a non-U.S. person because Section 401(a) applies only to non-U.S. person FISA targets, and the target is generally the person from whom, or about whom, information is sought. See FISA House Report at 73.

[20] 50 U.S.C. § 1803(a).

[21] 50 U.S.C. § 1804(a).

[22] 50 U.S.C. § 1805(a).

[23] Under current law, there are four situations in which electronic surveillance may be conducted without advance judicial approval: Under 50 U.S.C. § 1802; in an emergency situation under 50 U.S.C. § 1805(f); for training and testing under 50 U.S.C. § 1805(g); and immediately following a declaration of war by Congress under 50 U.S.C. § 1811.

[24] 50 U.S.C. § 1806(c).

[25] 50 U.S.C. §§ 1807-1808.

[26] 50 U.S.C. § 1809 (criminal liability); see 50 U.S.C. § 1810 (civil liability).

[27] 50 U.S.C. §§ 1801-1811.

[28] 50 U.S.C. § 1801(f)(1)-(4). The definition is unchanged from its enactment in 1978, except that the exclusion in subsection (2) for trespassers as defined in 18 U.S.C. § 2511(2)(i) was added by Section 217 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[29] 18 U.S.C. §§ 2510-2522.

[30] Subsections (1) and (2) of the definition apply to wire communications.

[31] Subsections (1) and (3) of the definition apply to radio communications.

[32] Subsection (4) of the definition applies to information that is neither a wire nor a radio communication.

[33] See Webster's Revised Unabridged Dictionary 287 (1913).

[34] Although FISA was enacted before the advent of commercially available e-mail, its legislative history makes clear that the statute "is not limited to the acquisition of the oral or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire." FISA House Report at 51. The FBI has revealed, in publicly available documents, that it has used FISA for "the interception of telephone and fax communications, and interception of e-mails." Affidavit of FBI Special Agent Randall Thomas, FBI, in support of application for complaint and arrest warrant for James J. Smith (available at http://news.findlaw.com/hdocs/docs/fbi/usleung403cmp.pdf).

[35] Compare 50 U.S.C. § 1801(f)(1)-(3), with 50 U.S.C. § 1801(f)(4). Cf. *Joao v. Sleepy Hollow Bank*, 348 F. Supp. 2d 120, 127 (S.D.N.Y. 2004) (discussing the term "communication device").

[36] Cf., e.g., *United States v. O'Brien*, 391 U.S. 367 (1968) (First Amendment symbolic speech analysis of burning a draft card).

[37] 50 U.S.C. § 1801(l).

[38] FISA House Report at 66.

[39] A possible argument against that conclusion would be to assert that the radio connection between a cordless or mobile handset and a base station or tower is a "like connection" – i.e., like a connection by wire – within the meaning of 50 U.S.C. § 1801(f)(1). However, the legislative history provides explicitly that "[a] radio signal is not within the term, a 'like connection,' in this definition," FISA House Report at 67, and it would be difficult to distinguish on these grounds the radio signal used by a cordless or mobile phone from all other radio signals (other distinctions, such as the use of encryption, would not be directly relevant to the question). Indeed, although commercial cordless and mobile telephones did not exist when FISA was enacted, the legislative history refers to a 1978 analogue: "ordinary marine band [radio] communications, which do not have a reasonable expectation of privacy or require a warrant for law enforcement interception, can be 'patched in' to telephone systems, becoming a 'wire communication.'" FISA House Report at 66. (This portion of the legislative history is actually a discussion of Title III, but the implication is that the marine radio telephone call would be a "wire communication" under FISA only insofar as it was "patched in" and traveling over the telephone system, but not while traveling between the marine radio and the point of reception that connects to the wired telephone system.)

[40] See FISA House Report at 52 (explaining that electronic surveillance of "radio communications" includes "not only the acquisition of communications made wholly by radio but also the acquisition of communications which are carried in part by wire and in part by radio, where the radio transmitted portion of those communications is intercepted"); S. Rep. No. 95-604 at 33. (1977) [hereinafter FISA Senate Judiciary Report].

[41] 18 U.S.C. § 2510(1).

[42] FISA House Report at 66 (contrasting FISA with Title III on this issue). But cf. H. R. Rep. No. 99-647 (1968), at 34 (noting that Title III's "definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication."). An "electronic communication" as defined by Title III may also travel by wire, but is not thereby rendered a "wire communication."

[43] 50 U.S.C. § 1801(l).

[44] Even after *United States v. Lopez*, 514 U.S. 549 (1995), and its progeny, Congress probably enjoys authority to regulate purely intrastate use of an interstate telecommunications facility. See, e.g., *Weiss v. United States*, 308 U.S. 321, 327 (1939) ("Congress has power, when necessary for the protection of interstate commerce, to regulate intrastate transactions."); see also S. Rep. No. 90-1097 at 92 (1968) (Senate report underlying Title III).

[45] FISA House Report at 66.

[46] Black's Law Dictionary at 87 (8th ed. 2004).

[47] 47 U.S.C. § 153(10); see 47 C.F.R. § 21.2; *National Association of Regulatory Utility Commissioners v. FCC*, 525 F.2d 630 (D.C. Cir. 1976); *Local Exchange Carriers' Rates, Terms & Conditions, for Expanded Interconnection*, 12 FCC Rcd 18730, ¶ 17 (1997); see generally *FCC v. Midwest Video Corp.*, 440 U.S. 689, 701 (1979) (defining a common carrier as an entity that "makes a public offering to provide [communications facilities] whereby all members of the public who choose to employ such facilities may communicate or transmit intelligence of their own design and choosing" (internal quotation marks and citations omitted)). As explained in the text, Title III cross-references the statutory definition in the Communications Act. 18 U.S.C. § 2510(10).

[48] Although Title III defines the term "communication common carrier," the definition no longer plays a significant part in Title III's statutory scheme. It is not part of Title III's definitions of "wire communication," see 18 U.S.C. § 2510(1), or "electronic communication," see 18 U.S.C. § 2510(12). As amended in 1970, Title III required a "communication common carrier" to assist the government in implementing a Title III court order under certain circumstances. See *Dalia v. United States*, 441 U.S. 238, 270 n.19 (1979) (Stevens, J., dissenting). However, following amendments made in 1986 (by ECPA), Title III today requires assistance from a "provider of wire or electronic communication service." 18 U.S.C. § 2518(4); see *In re Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications*, 349 F.3d 1132, 1136-1137 & n.8, 1139 & n.13 (9th Cir. 2003). "By amending the statute, Congress undeniably intended to expand the scope of the provision to cover more than common carriers." *Id.* at 1139 n.13. The changes to Title III may suggest the need for an amendment to FISA's definition of "wire communication" if the government's proposal does not pass; FISA secondary electronic surveillance orders can be issued not only to a "common carrier," but also to any "other specified person." 50 U.S.C. § 1805(c)(2)(B); cf. *In re Application of the U.S.*, 349 F.3d at 1141-1143 (discussing "other person" as used in Title III).

[49] The 1978 House Report on FISA explains that "one of the committee's purposes has been to produce legislation that can be read and understood (and thus complied with) easily, without excessive cross reference to other statutes." FISA House Report at 98. To the extent that FISA requires cross-reference to the Communications Act with respect to the meaning of "common carrier," it tends to frustrate that purpose.

[50] See, e.g., *National Communications Ass'n, Inc. v. A.T.&T Corp.*, 238 F.3d 124, 125 (2d Cir. 2001).

[51] See 47 U.S.C. § 332(c)(1)(A).

[52] 47 U.S.C. § 541(c). For the FCC's definition of a "cable television system," see 47 C.F.R. § 76.5; see also 47 U.S.C. § 522(7). The definition of "wire communication" in FISA includes signals while being carried by a "cable" as well as a "wire." 50 U.S.C. § 1801(l).

[53] The FCC has not yet determined whether providers of VOIP are common carriers under the Communications Act. See IP-Enabled Services, Notice of Proposed Rulemaking, 19 FCC Rcd 4863, ¶ 43 (2004) (regarding VoIP). The FCC explains that "VoIP allows you to make telephone calls using a computer network, over a data network like the Internet. VoIP converts the voice signal from your telephone into a digital signal that travels over the internet then converts it back at the other end so you can speak to anyone with a regular phone number. When placing a VoIP call using a phone with an adapter, you'll hear a dial tone and dial just as you always have. VoIP may also allow you to make a call directly from a computer using a conventional telephone or a microphone." See www.fcc.gov/voip/. However, interpreting and applying the Communications Assistance to Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-1021, the FCC has publicly mandated that VOIP providers configure their systems to

aid wiretapping by the federal government. www.fcc.gov.wcb/iatd/calea.html. For a discussion of this mandate by (among others) a former NSA official, see http://itaa.org/news/docs/CALEAVOIPreport.pdf.

[54] *NCTA v. Brand X Internet Services*, 545 U.S. 967 (2005). "Shortly after the *Brand X* decision, the FCC convened its Open Commission Meeting on August 5, 2005, and adopted a policy that both DSL and cable modem services are information services and not subject to common carrier regulation." Anna Zichterman, Note, *Developments In Regulating High-Speed Internet Access: Cable Modems, DSL, & Citywide Wi-Fi*, 21 Berk. T. LJ 593, 604 (2006) (citing *In re Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 F.C.C.R. 14853, 14871-72 (2005) (available at http://hraunfoss.fcc.gov/edocs_ public/attachmatch/FCC-05-150A1.pdf); Press Release, FCC Eliminates Mandated Sharing Requirement on Incumbents' Wireline Broadband Internet Access Services (Aug. 5, 2005) (available at http:// hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf)).

[55] See, e.g., *Howard v. America Online, Inc.*, 208 F.3d 741, 752-753 (9th Cir. 2000).

[56] See *Brand X*, 545 U.S. at 973-974.

[57] For NASA's description of wavelengths and the electromagnetic spectrum (targeted at students in grades 5-8, but also within the grasp of most lawyers), see www.nasa.gov/audience/forstudents/5-8/features/F_The_Electromagnetic_Spectrum.html.

[58] See FISA House Report at 52 (referring to a ham radio or CB signal).

[59] See *id.* at 52 ("It is the committee's intent that the intentional acquisition of the contents of a communication being transmitted by common carrier radio microwave ... would clearly be included here"), 67 ("Interception of microwave communications carried by common carriers, by intercepting the radio signal, is electronic surveillance").

[60] However, the FCC explains that microwaves are "in the upper range of the radio spectrum." See http://wireless.fcc.gov/microwave/.

[61] FISA House Report at 52. See *United States v. Karo*, 468 U.S. 705 (1984). In some situations, there is no reasonable expectation of privacy in the location of an object or vehicle – e.g., when a vehicle is on the open road and subject to physical surveillance. But information about location is a type of information that may be acquired via "electronic surveillance," depending on the circumstances. Where a radio communication is unintentionally acquired, it generally must be destroyed. See 50 U.S.C. § 1806(i).

[62] Under 50 U.S.C. § 1801(f)(3), concerning radio communications, the acquisition must be "[i]ntentional." The legislative history explains that "by their very nature, radio transmissions may be intercepted anywhere in the world, even though the sender and all intended recipients are in the United States [an element of "electronic surveillance" as defined by Subsection (3)]. Thus, intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of [radio] communications intended to be totally domestic." FISA House Report at 52. By negative implication, this suggests that accidental acquisition may qualify as "acquisition" under the remaining three subsections of current 50 U.S.C. § 1801(f).

[63] While FISA uses the term "acquisition" and Title III uses the term "interception" to describe surveillance, the latter statute defines "interception" as "the aural or other *acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). Perhaps for that reason, FISA's legislative history sometimes uses the terms interchangeably. See, e.g., House Report at 55 ("By minimizing acquisition, the committee envisions, for example, that in a given case, where *A* is the target of the wiretap, after determining that *A*'s wife is not engaged with him in clandestine intelligence activities, the interception of her calls on the tapped phone, to which *A* was not a party, probably ought to be discontinued as soon as it is realized that she rather than *A* was the party").

[64] See *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994); see also *United States v. Lewis*, 406 F.3d 11, 17 n.5 (1st Cir. 2005); cf. *United States v. Hammoud*, 286 F.3d 189, 192-193 (4th Cir. 2002). The Ninth Circuit

appears to have held that the routine recording of incoming calls by a sheriff's office is not "interception" under Title III because it does not involve "active surveillance." *Greenfield v. Kootenai County*, 752 F.2d 1387 (9th Cir. 1985). Whatever the merits of Greenfield's reasoning with respect to Title III, it seems dubious as applied to FISA. Cf. *Ariasi v. Mutual Central Alarm Service, Inc.*, 202 F.3d 553, 557-558 (2d Cir. 2000) (noting that "[t]he case law with respect to Title III is somewhat unclear regarding the proper definition of an 'interception' under the statute" and citing and discussing cases).

[65] See, e.g., Glenn A. Fine, Department of Justice Inspector General, *Top Management Challenges in the Department of Justice* (2004) (noting that "the FBI's collection of material requiring translation outpaced its translation capabilities and the FBI did not translate all the foreign language counterterrorism and counterintelligence material it collected," and that "the FBI's digital collection systems have limited storage capacity and consequently unreviewed audio sessions are sometimes deleted automatically to make room for incoming audio sessions") (available at www.usdoj.gov/oig/challenges/2004.htm).

[66] See Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, FBI, Before the United States Senate Committee on the Judiciary (Sept. 6, 2000) (available at www.fbi.gov/congress/congress00/kerr090600.htm).

[67] *Id.*

[68] That accords with FISA's use of "acquisition" in the definition of "minimization procedures." 50 U.S.C. § 1801(h)(1). Under Defense Department regulations, information is "collected" when it has been "received for use by an employee of a DoD intelligence component," and "[d]ata acquired by electronic means is 'collected' only when it has been processed into intelligible form." Department of Defense, DOD 5240 1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons* § C.2.2.1 (Dec. 1982) (available at www.dtic.mil/whs/directives/corres/text/d52401p.txt) [hereinafter DOD 5240 1-R]; see also National Security Agency, United States Signals Intelligence Directive 18 § 9.2 (July 1993) (available at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm) [hereinafter USSID-18].

[69] This phrase appears in all four subsections of current 50 U.S.C. § 1801(f).

[70] 18 U.S.C. § 2510(5).

[71] See 18 U.S.C. § 2511.

[72] 50 U.S.C. §§ 1809, 1810.

[73] FISA House Report at 53.

[74] *United States v. Dubrofsky*, 582 F.2d 208, 211 (9th Cir. 1978) (holding that these techniques are not "searches" within the meaning of the Fourth Amendment). See *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that a dog sniff is not a Fourth Amendment "search").

[75] Compare *Kyllo v. United States*, 533 U.S. 27 (2001) (use of sense-enhancing technology to gather information regarding the interior of a home that could not otherwise have been obtained without a physical intrusion into a constitutionally protected area constitutes a "search" for Fourth Amendment purposes), with, e.g., *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (aerial photography of a business not a Fourth Amendment "search").

[76] Cf. *Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search – at least where (as here) the technology in question is not in general public use" (citations omitted)).

[77] 18 U.S.C. § 2512(1)(b) (prescribing punishment for anyone who "manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it

primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce").

[78] The cases are collected in Tammy Hinshaw, *What Constitutes "Device Which Is Primarily Useful for the Surreptitious Interception of Wire, Oral, or Electronic Communication," Under 18 U.S.C.A. § 2512(1)(B), Prohibiting Manufacture, Possession, Assembly, Sale of Such Device*, 129 A.L.R. Fed. 549 (2004).

[79] See, e.g., *United States v. Schweihs*, 569 F.2d 965 (5th Cir. 1978).

[80] See S. Rep. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2183-84 ("The prohibition will thus be applicable to, among others, such objectionable devices as the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack.").

[81] 50 U.S.C. § 1801(n).

[82] 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").

[83] Thus, it includes the information acquired by pen/trap surveillance. Section 401(e) of the government's proposal would change the definition of "contents" in FISA.

[84] See FISA House Report at 67.

[85] 50 U.S.C. § 1801(f)(2), (4).

[86] 50 U.S.C. § 1801(j).

[87] Cf. *Rasul v. Bush*, 124 S. Ct. 2686, 2696 (2004).

[88] FISA House Report at 65.

[89] *Salisbury v. United States*, 690 F.2d 966, 968-969 (D.C. Cir. 1982) (citations omitted, ellipsis in original). As described here, the technology used in NSA watchlisting is different from the technology used in the FBI's Carnivore system. While NSA intercepted all communications on a monitored channel, and then later discarded any intercepted communications that were not responsive to a watch list, Carnivore effectively combines the two steps, capturing communications in a computer's random access memory and discarding them before they are recorded to a hard drive or other permanent media if they do not meet the criteria established by the device's programming. For a more complete discussion of watchlisting and FISA, see House FISA Five Year Report at 5-6.

[90] See, e.g., *Ring v. Arizona*, 536 U.S. 584, 620 & n.1 (2002) (O'Connor, J., dissenting) (referring to a Westlaw search); *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003) (vacating discovery order allowing tort plaintiff unlimited access to Ford's databases without designating search terms to restrict the search).

[91] FISA House Report at 51 (emphasis added). One rationale for this may have been to avoid civil liability for accidental interceptions. Cf. FISA Senate Judiciary Report at 33-34 (discussing use of "intentional" standard in Subsection (3) of the current definition of "electronic surveillance").

[92] 50 U.S.C. § 1801(j).

[93] Subsection (2) of the current definition of "electronic surveillance" applies only when no party to the communication has consented to the surveillance.

[94] 389 U.S. 347, 360-362 (1967).

[95] See, e.g., *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

[96] FISA House Report at 54.

[97] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 272-273 (1990). In his dissenting opinion in *Verdugo-Urquidez*, Justice Brennan stated that "[n]umerous lower courts ... have held that illegal aliens in the United States are protected by the Fourth Amendment, and not a single lower court has held to the contrary." *Id.* at 283 n.6 (Brennan, J., dissenting) (citing cases).

[98] FISA House Report at 54.

[99] 50 U.S.C. § 1801(f)(1), (3), (4) (emphasis added).

[100] Subsection (1) of the current definition refers to acquisition of a communication sent to or from "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." Subsection (2) of the current definition refers to acquisition of the contents of any wire communication "to or from a person in the United States, without the consent of any party thereto." Current Subsection (3) refers to intentional acquisition of a communication "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States." And current Subsection (4) refers to acquiring information "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(1)-(4). Had Congress intended a narrower approach, the more natural phrasing would have been "that person" (i.e., the targeted person), in Subsection (1), "a party" to the communication in Subsection (2), "the sender and all intended recipients" of the communication in Subsection (3), and "the target" of the surveillance in Subsection (4).

[101] 50 U.S.C. § 1821(5).

[102] See 50 U.S.C. § 1822(c) (FISC has jurisdiction to issue orders authorizing physical searches).

[103] See *Minnesota v. Carter*, 525 U.S. 83 (1998); cf. *Steagald v. United States*, 451 U.S. 204 (1981) (absent consent or exigent circumstances, government may not search for the subject of an arrest warrant in the home of a third party without a search warrant for the third party's home). See generally *Stanford Daily v. Zurcher*, 436 U.S. 547 (1978) (upholding warrants directed at third parties who possess evidence of a defendant's crime). Even if the defendant in a criminal case cannot invoke the exclusionary rule in such a case – because he individually lacks a reasonable expectation of privacy – the existence of a reasonable expectation of privacy held by any person in the place to be searched requires adherence to Fourth Amendment requirements. Similarly, under current Subsections (1), (3), and (4), and the current definition of "physical search," a FISC order is normally required where a search or surveillance would infringe on any person's reasonable expectation of privacy (and the other elements of the definitions and the statute are met).

[104] FISA House Report at 53.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] See FISC R. 10(A)(i) (available at www.uscourts.gov/rules/FISC_Final_Rules_Feb_2006.pdf).

[109] The analogous element in current Subsection (2) is "the consent of any party" to an intercepted communication.

[110] *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973).

[111] *United States v. Robinson*, 414 U.S. 218 (1973); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (allowing search incident to arrest of a pager because pager data is transient).

[112] *Carroll v. United States*, 267 U.S. 132 (1925).

[113] *South Dakota v. Opperman*, 428 U.S. 364 (1976).

[114] As discussed elsewhere in these comments, an e-mail user may have no reasonable expectation of privacy in an e-mail sent through his ISP, but if the ISP is an "electronic communications service" as defined by Title III and Chapter 206 of Title 18, the government will need a warrant to compel production of the e-mail if it is less than six months old and has not yet been read. Under 18 U.S.C. § 2703(a), "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant."

[115] There is no reasonable expectation of privacy in the "routing and addressing" information obtained by pen/trap surveillance (at least when obtained from a third party), see *Smith v. Maryland*, 442 U.S. 735 (1979), but the government cannot get such information for law enforcement purposes without a pen/trap order from a district court. A pen/trap order may not be a "warrant" within the meaning of 50 U.S.C. § 1801(f), however, because it does not require a showing of probable cause. Either way, pen/trap surveillance of wire communications, conducted in the United States, of any person in the United States, is "electronic surveillance" under current FISA absent consent, because current Subsection (2) does not depend on the existence of a reasonable expectation of privacy or the need for a warrant. See 50 U.S.C. § 1801(f)(2).

[116] Pub. L. 107-56, § 1003, 115 Stat. 272, 392 (Oct. 26, 2001).

[117] Section 2511(2)(i) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if –
>
> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;
>
> (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
>
> (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.
>
> The term "protected computer" means a computer –
>
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

18 U.S.C. § 2510(20) and 18 U.S.C. § 1030(e)(2).

> The term "computer trespasser" –
>
> (A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
>
> (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. § 2510(21).

[118] This provision is limited to such communications as defined by Title III, not FISA.

[119] In some cases, a hacked computer is used as a pass-through to reach a third computer that the hacker is exploiting, the owner of the pass-through computer probably would not be a "party" to the hacker's communication with the third, exploited computer, and so the provision could make a difference.

[120] To the extent that they are exempt from regulation under FISA, such communications are also exempt from regulation under Title III. A provision of Title III provides specifically that "[n]othing contained in this chapter [18 U.S.C. §§ 2510-2522] or chapter 121 [the Stored Communications Act, 18 U.S.C. §§ 2701-2712] or 206 [the pen/trap provisions of 18 U.S.C. §§ 3121-3127] of this title, or section 705 of the Communications Act of 1934 [47 U.S.C. § 605], 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." 18 U.S.C. § 2511(2)(f). See also 50 U.S.C. § 1821(5) (similar exemption in FISA's current definition of "physical search").

[121] Current Subsection (1) applies only to wire and radio communications involving "a particular, known United States person who is in the United States." Subsection (2) applies only to wire communications "to or from a person in the United States." Subsection (3) applies only to radio communications "if both the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(1)-(3).

[122] Current Subsection (4) requires the "installation or use" of a surveillance device "in the United States." If one or more of the parties to a communication were standing just outside the U.S. border, and the government used a boom microphone to record at least one side of the communication from just inside the border, it would be "electronic surveillance" under current Subsection (4) because the surveillance device – the microphone – would be used inside the U.S.

[123] Nor would Title III apply in that situation. See, e.g., *United States v. Barona*, 56 F.3d 1087, 1090 (9th Cir. 1995) ("When determining the validity of a foreign wiretap, we start with two general and undisputed propositions. The first is that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-21, 'has no extraterritorial force'"); *United States v. Peterson*, 812 F.2d 486, 492 (9th Cir. 1987) (citing cases for the proposition that Title III has no extraterritorial application); see generally, e.g., *EEOC v. Arab American Oil Co.*, 499 U.S. 244 (1991) (general presumption against extraterritorial application of U.S. statutes). In general, no U.S. court can issue an ordinary search warrant for a foreign jurisdiction. See *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[124] FISA House Report at 51.

[125] Cf. 18 U.S.C. § 2511(2)(g) ("It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system").

[126] Cf. *United States v. Smith*, 978 F.2d 171, 179 (5th Cir. 1992) ("cordless phones now appearing on the market actually scramble the radio signal so that even radio scanners cannot intercept the communication").

[127] 50 U.S.C. § 1822(c).

[128] 50 U.S.C. § 1823.

[129] 50 U.S.C. § 1824.

[130] 50 U.S.C. § 1822(a).

[131] 50 U.S.C. § 1825.

[132] 50 U.S.C. § 1826.

[133] 50 U.S.C. §§ 1827 (criminal liability), 1828 (civil liability).

[134] Under 50 U.S.C § 1821(1), the term "United States" has the same meaning in the context of a physical search as it does in the context of electronic surveillance.

[135] 533 U.S. 27 (2001).

[136] As the Court explained in *Kyllo*, "[t]hermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth – black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images." *Id.* at 29-30.

[137] *Id.* at 30.

[138] *Id.* at 31.

[139] *Id.* at 31-32 (internal quotations omitted).

[140] *Id.* at 33.

[141] *Id.* at 34 (internal quotations and citation omitted).

[142] *Id.* at 32 n.1 (quoting N. Webster, *An American Dictionary of the English Language* 66 (1828)).

[143] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (footnote omitted).

[144] H.R. Conf. Rep. No. 103-753 at 80 (1994) [hereinafter FISA Search Conference Report].

[145] 50 U.S.C. § 1801(f)(4).

[146] 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter ... shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications ... utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978").

[147] FISA House Report at 100. As the Senate Judiciary Report underlying FISA went on to explain, citing to the Church Committee reports on abuses by the government, "[t]he activities of the National Security Agency pose particularly difficult conceptual and technical problems which are not dealt with in this legislation." S. Rep. No. 95-604 at 64 (1977).

[148] In 1986, Congress concluded that there is no reasonable expectation of privacy in cordless telephone calls because the radio signals broadcast by such telephones can be intercepted easily, and therefore exempted their interception from regulation under Title III. Electronic Communications Privacy Act (ECPA), Pub. L. No. 508, 99th Cong., 2d Sess., § 101(a)(1)(D), 100 Stat. 1848 (1986) (adding the following to the definition of "wire communication" in Title III: "such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit"). As the Senate Report underlying ECPA explained, "[b]ecause communications made on some cordless telephones can be intercepted easily with readily available technologies, such as an AM radio, it would be inappropriate to make the interception of such a communication a criminal offense." S. Rep. No. 99-541 at 12 (1986). In 1994, however, Congress eliminated the exemption, bringing cordless telephone transmissions within the scope of Title III. See Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 414, 103rd Cong., 2d Sess. § 202(a), 108 Stat. 4279 (1994) (deleting the language added by ECPA). As the House Report underlying CALEA explained, a privacy and technology task force examined "the newer generation of cordless phones" and recommended that "the legal protections of ECPA be extended" to cover them; the task force found that "'[t]he cordless phone, far from being a novelty item used only at 'poolside,' has become ubiquitous ... More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call.' Therefore, [CALEA] includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority." H.R. Rep. No. 103-827 at 12, 17 (1994) (last ellipsis in original).

The courts of appeals have not authoritatively resolved the reasonableness of an expectation of privacy in the radio signal emitted by cordless telephones. See, e.g., *Frieerson v. Goetz*, 99 Fed. Appx. 649, 2004 WL 1152172 (6th Cir. May 19, 2004) (unpublished decision) (granting qualified immunity for unauthorized interception of cordless telephone radio signal). However, it may be that expectations of privacy in newer generations of cordless telephones, used after CALEA, will be found to be reasonable, even if that is not the case for older models used before CALEA. See, e.g., *Price v. Turner*, 260 F.3d 1144, 1148 (9th Cir. 2001) ("At the time of Price's cordless phone conversations [1989-1991], they were readily susceptible to interception. For that very reason, the transmissions were not protected by the Wiretap Act. Price cannot be said to have had an objectively reasonable expectation of privacy in those communications"); *United States v. Smith*, 978 F.2d 171, 180 (5th Cir. 1992) ("as technological advances make cordless communications more private at some point such communication will be entitled to Fourth Amendment protection. Given this conclusion, it should be equally obvious that it is not enough for a trial court to conclude that interception of a conversation does not implicate Fourth Amendment concerns simply because it is carried by a 'cordless' phone. Application of the Fourth Amendment in a given case will depend largely upon the specific technology used").

[149] See, e.g., *Katz v. United States*, 389 U.S. 347 (1967); 18 U.S.C. §§ 2510-2522.

[150] FISA House Report at 50 (emphasis in original).

[151] Thus, for example, the kind of surveillance alleged to have taken place in *Blind Man's Bluff*, in which the U.S. Navy tapped an undersea telephone cable used to carry communications between Soviet military officials outside the United States, would not be regulated by FISA. Sherry Sontag & Christopher Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage* (Harper 1998).

[152] One argument against this conclusion is that acquisition of the contents of a radio communication is electronic surveillance under subsection (3) if the "sender and all intended recipients" of the radio communication itself are in the United States. On that argument, the "recipient" of the radio communication is the cordless telephone's base station; the other human party to the telephone call is the recipient only of the (international) wire communication that begins after the (domestic) radio communication arrives at the cordless telephone base station. This argument, however, seems quite strained. When FISA was enacted in 1978, as discussed in the text, the radio portions of international telephone calls (made by non-U.S. persons) were exempt from regulation. See FISA Senate Judiciary Report at 34.

[153] Under 18 U.S.C. § 2510(1) and (12), a "wire communication" is an "aural" transfer, and an "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature" other than a wire or oral communication. A fax is an "electronic communication" under Title III.

[154] One difference is that a fax, unlike a telephone call, generates a permanent record of its contents – the paper that comes out of the recipient's fax machine. Acquisition of the contents of this paper after it has been removed from the fax machine would be treated like the acquisition of any other paper under FISA. The fact that it had been sent by fax would be irrelevant if the acquisition occurred after it was out of the fax machine.

[155] For example, the Global System for Mobile Communications (GSM) protocol is generally used in Europe (and elsewhere).

[156] Instead, they would be regulated by Section 2.5 of Executive Order 12333.

[157] The basics of e-mail and voice mail protocols, and the ways in which they differ from traditional telephone protocols, are not too difficult to grasp. Here is how the government described e-mail in a brief filed in the First Circuit in November 2004:

> e-mail is an electronic transfer of a message from one computer user to another. An e-mail message typically travels through a series of computers as it goes from sender to receiver. The sender creates the e-mail message using an e-mail program and directs the program to send the message. Once sent, the message travels from the sender's computer to the sender's e-mail service provider. The provider's computer accepts the message using a program called a "Message Transfer Agent" (MTA), saving the message to either the computer's random access memory (RAM) or its hard drive. The MTA forwards the accepted message out through the Internet to yet another computer, which then repeats the process of using an MTA to accept and forward the message to another computer, and so on. This process of passing a message from computer to computer is known as the "store-and-forward" process. The computer-to-computer transmission continues until the MTA at the recipient's e-mail service provider accepts the message and stores it in a location accessible to the recipient, that is, his inbox. This is known as "final delivery," and is often achieved with the assistance of a program called a "Message Delivery Agent" (MDA).

Supplemental Brief for the United States, *United States v. Councilman*, No. 03-1383 (1st Cir. Nov. 4, 2004), 2004 WL 3201458. For a more complete discussion of e-mail and the Internet, see http://computer.howstuffworks.com/email.htm.

As this excerpt reveals, there is an argument that an e-mail message consists of not one, but several discrete "communications." At the most basic level, ignoring the actual complexity of the Internet, the first communication would be between the sender and his own ISP, the next would be between the sender's ISP and the recipient's ISP (or any intermediate computers), and the last would be between the recipient's ISP and the recipient as he downloads the e-mail onto his personal computer. That is not, however, how the courts have analyzed e-mail communications under criminal law surveillance provisions. See *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) ("We conclude that the term 'electronic communication' [as used in Title III] includes transient electronic storage that is intrinsic to the communication process for such communications").

[158] As the First Circuit explained in *Councilman*:

> There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes.

418 F.3d at 76 (quoting Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties (*available at www.wws.princeton.edu/ ota/disk2/1985/8509_ n.html (Oct.1985))).

[159] For a discussion of POTS, see http://electronics.howstuffworks.com/telephone.htm.

[160] By contrast, a traditional telephone call does not leave footprints of its content in the telecommunications network. There is no content to be acquired either before the parties to a call connect, or after they hang up. Thus, electronic surveillance of such a telephone call is possible, if at all, only in real time, when the call is either a wire or radio communication. That is how the courts of appeals have interpreted the corresponding provisions in Title III. See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2004) ("every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission of the electronic communication"); *United States v. Steiger*, 318 F.3d 1039, 1048-1049 (11th Cir. 2003) ("a contemporaneous interception – i.e., an acquisition during 'flight' – is required to implicate the Wiretap Act with respect to electronic communications"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 459-460 (5th Cir. 1994).

[161] Voice mails are entrusted to and stored by third parties only if stored by the telephone company as part of a voice-mail service, not if they are simply recorded on a stand-alone home answering machine.

[162] 50 U.S.C. § 1801(l).

[163] That would be the case unless an ISP's e-mail server were treated as a "wire" that is "carry[ing]" the e-mail it stores, which seems implausible.

[164] 50 U.S.C. § 1801(f)(1)-(3).

[165] 50 U.S.C. § 1801(f)(4).

[166] Similarly, acquisition of stored communications from a target's personal computer, or his home answering machine, could also involve a "surveillance device," again depending on the facts. If a government agent simply enters a target's home and listens to his voice mail, or copies e-mail from his personal computer's hard drive to a CD or other portable storage media, it probably would not qualify as "electronic surveillance" under Subsection (4) because the acquisition does not involve a "device," as discussed above. (It could, however, qualify as a "physical search.") However, a concealed microphone that overhears a voice mail being played by the target, or a concealed video camera that records a computer screen while an e-mail is displayed on it, would be a "surveillance device" under Subsection (4).

[167] 50 U.S.C. § 1821(5) provides that a physical search "does not include ... 'electronic surveillance', as defined in section 1801(f)." Thus, acquisition of stored communications can be a "physical search" only if it has been found not to be "electronic surveillance." The distinction between treating acquisition of stored communications as a search rather than surveillance may have little impact on civil liberties, but it may be significant to certain members of the Intelligence Community – for example, under the publicly available version of Executive Order 12333, the NSA may conduct electronic surveillance, but may not conduct physical searches, inside the United States.

[168] 50 U.S.C. §§ 1801(f)(4) (electronic surveillance), 1821(5) (physical search).

[169] See *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

[170] 18 U.S.C. §§ 2702(a)(1), 2703(a). Ordinarily, information held by third parties is subject to subpoena, and so a warrant might not be necessary. See generally *United States v. R. Enterprises*, 498 U.S. 292 (1991); cf. *Hale v. Henkel*, 201 U.S. 43, 76-77 (1906) (using Fourth Amendment to determine "reasonableness" of a subpoena). By statute, 18 U.S.C. § 2703(b), communications held in storage for more than 180 days may be acquired by warrant or subpoena, among other methods. Thus, acquisition of these older communications is not governed by FISA.

[171] Under 18 U.S.C. § 2510(15), which applies here pursuant to 18 U.S.C. § 2711(1), an "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." The legislative history explains that "telephone companies and electronic mail companies are providers of electronic communication services." S. Rep. No. 99-541 at 14 (1986).

[172] Under 18 U.S.C. § 2510(17), which applies here pursuant to 18 U.S.C. § 2711(1), the term "electronic storage" means either "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"; or "(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The precise meaning of this provision remains uncertain. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc). The Department of Justice, which supported rehearing in *Councilman*, acknowledges that "e-mail that has been received by a recipient's service provider but has not yet been accessed by the recipient is in 'electronic storage,'" but maintains that it is not in such storage after "the recipient retrieves the e-mail." DOJ's argument is that retrieved e-mail is "no longer in 'temporary, intermediate storage ... incidental to ... electronic transmission.'" Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Part III.B (July 2002) (available at www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#_IIIB_).

Whatever the merits of these arguments, it seems clear that unread e-mail less than six months old, held on the server of the sender or recipient's ISP, is in "electronic storage." Such storage will almost always be in an "electronic communications system" because that term is defined broadly to mean "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14) (applicable here pursuant to 18 U.S.C. § 2711(1)). As a practical matter, because the government cannot know in advance when a recipient will retrieve any particular e-mail, and because it obviously prefers to read a suspected terrorist's e-mail before the terrorist himself does so, it must effectively proceed in all cases as if bound by the restrictions.

[173] 442 U.S. 735 (1979). Although *Smith v. Maryland* was decided several months after FISA's enactment, Congress seems to have anticipated its holding, because it understood that pen/trap surveillance would be "electronic surveillance" under 50 U.S.C. § 1801(f)(2), the part of the definition that does not require a reasonable expectation of privacy. See FISA House Report at 51. Under Subsection (2), pen/trap surveillance conducted in real time is "electronic surveillance" where the "acquisition" occurs in the United States (i.e., the surveillance is conducted in the United States), and at least one party to the communication is in the United States, unless a party consents to the surveillance.

[174] *Smith*, 442 U.S. at 743 (citations omitted).

[175] 425 U.S. 435 (1976).

[176] See also *Couch v. United States*, 409 U.S. 322, 335-336 & n.19 (1973) (no reasonable expectation of privacy in financial papers provided to an accountant). Decisions such as *Hoffa v. United States*, 385 U.S. 293, 302 (1966), which upheld the practice of consensual monitoring, should be distinguished because they hold only that any party to a private communication may consent to law enforcement monitoring of the communication. The sender retains a reasonable expectation of privacy in such communications despite the possibility that the recipient may consent, and absent consent a warrant is still required. By contrast, when an otherwise private communication is conveyed and made available to third parties, *Smith* and *Miller* can be read to hold that the reasonable expectation of privacy is simply lost. The Court has not always maintained the distinction, however, perhaps because, as a practical matter, the third party's consent or a warrant or subpoena is usually required for the government to get access to the

information because the third party's reasonable expectation of privacy in the place where the information is being kept. See, e.g., *Miller*, 425 U.S. at 440 (citing Hoffa). This fact is critical under FISA.

[177] 442 U.S. at 743.

[178] *Id.* at 743-744 (citations omitted). In *Miller*, the Court stated that it "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S. at 443.

[179] As the Senate Report underlying Chapter 121 explains (S. Rep. No. 99-541 at 3 (1986) (footnote omitted)):

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. See *United States v. Miller*, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

[180] See 18 U.S.C. § 2702(b)(6) (allowing electronic communications service provider to disclose the contents of a communication to the National Center for Missing and Exploited Children without a warrant or consent). Under 42 U.S.C. § 13032(b)(1), if an electronic communication service provider "obtains knowledge of facts or circumstances from which a violation of [certain criminal statutes] involving child pornography ... is apparent," then it "shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General." (Perhaps this provision could be defended based on one of the warrant exceptions to the Fourth Amendment, but it seems unlikely.)

[181] For example, the Court could distinguish *Miller* on the ground that "the documents subpoenaed here are not respondent's 'private papers,'" and perhaps also on the ground that, assuming defendants' own documents were involved, "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions." 425 U.S. at 440, 442. The Court could distinguish *Smith* on the ground that it did not involve the "contents" of a communication. Moreover, as commentators have noted, there are reasons to doubt the reasoning of *Miller*. See, e.g., Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 Berkley Tech. L. J. 1283, 1292 & n.45 (2005) (criticizing *Miller*).

[182] *Miller* rejected a similar argument based on the Bank Secrecy Act.

[183] In *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F.), the Court of Appeals for the Armed Forces held that an AOL account holder had a reasonable expectation of privacy in the e-mails he sent through AOL, in part because "AOL's policy was not to read or disclose subscribers' e-mail to anyone except authorized users, thus offering its own contractual privacy protection in addition to any federal statutory protections."

[184] See, e.g., *Kyllo*, 533 U.S. at 31 (Scalia, J.).

[185] Compare, e.g., *California v. Greenwood*, 486 U.S. 35 (1988) (no reasonable expectation of privacy in garbage left on the curb for pickup by trash collector), with, e.g., *Ex parte Jackson*, 96 U.S. (6 Otto) 727, 733 (1878)

(reasonable expectation of privacy in sealed, first-class mail); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) (same). Unlike a letter, an e-mail is not sealed, but some ISPs have policies or contractual arrangements under which they do not read or disclose subscribers' e-mails.

[186] The cases in this area are collected in Mitchell Waldman, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15 (2004).

[187] 50 U.S.C. § 1801(f)(4).

[188] See 18 U.S.C. § 2702.

[189] If such acquisition of stored e-mail is a "physical search" (rather than "electronic surveillance") under FISA, however, there may be a question about the intersection with the Stored Communications Act, which (like Title III) generally prohibits disclosure of certain stored communications and also provides for certain exemptions. Under 18 U.S.C. § 2511(2)(e), neither the Stored Communications Act nor any other provision of Title 18 of the U.S. Code makes it "unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." There is no corresponding exemption, however, for physical searches under FISA. Under 18 U.S.C. § 2511(2)(f), the Stored Communications Act "shall [not] 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." This could in theory apply to FISA physical searches, because they are a means other than electronic surveillance as defined in FISA, but certainly would not apply to physical searches of a domestic ISP to obtain domestic e-mail messages. This exemption was adopted in 1978 to protect certain signals intelligence activities of the National Security Agency. See FISA House Report at 100.

[190] 18 U.S.C. § 2511(2)(c).

[191] This assumes that "a person" has a reasonable expectation of privacy that is implicated by the circumstances under which the government conducts the surveillance, as would be the case when the government enters the premises of the ISP.

[192] Current Subsection (1) could also apply if the target were a U.S. person, but where – as here – the acquisition of e-mail occurs in the United States, Subsection (2) is effectively broader in scope than Subsection (1). In particular, current Subsection (2) does not depend on the existence of a reasonable expectation of privacy or the need to use a warrant for law enforcement purposes, but only on the absence of consent from a party to the acquired communication (or applicability of the computer-trespasser exception from Title III).

[193] If neither party to the e-mail were located in the United States, then acquisition would not be regulated under current Subsection (2), but acquisition of e-mail to or from a U.S. person abroad would be governed by Section 2.5 of Executive Order 12333.

[194] The executive branch has maintained that the President has inherent authority to conduct electronic surveillance (in the non-technical sense) for national security purposes involving foreign powers or their agents, and could advance the argument that such power cannot be restrained by Congress, at least in certain circumstances.

[195] 18 U.S.C. § 2511(2)(e).

[196] 18 U.S.C. § 2511(2)(f).

[197] FISA House Report at 100.

[198] Letter from Lt. Gen. Keith Alexander, Director, NSA, to Senator Arlen Specter, Chairman, Committee on the Judiciary, U.S. Senate (19 December 2006) (Answer to Question 2a: "When FISA was enacted into law in 1978,

almost all transoceanic communications into and out of the United States were carried by satellite and those communications were, for the most part, intentionally omitted from the scope of FISA"). Subsection (2) of the current definition of "electronic surveillance" applies to radio communications, but only when the sender and all intended recipients are located in the United States. Subsection (1) of the current definition also applies to radio communications, but only when the surveillance targets a U.S. person in the United States.

[199] The Senate Judiciary Committee's report on FISA explains that "either a wholly domestic telephone call *or an international telephone call* can be the subject of electronic surveillance" – if acquired from a wire in the U.S. or from targeting a U.S. person in the U.S. – but that "most [international] telephonic and telegraphic communications are transmitted at least in part by microwave radio transmissions," leaving them open to surveillance outside FISA if acquired from the radio transmission without targeting a U.S. person in the U.S. FISA Senate Judiciary Report at 33 (emphasis added).

[200] The "directed at" formulation is used elsewhere in FISA, see, *e.g.*, 50 U.S.C. §§ 1802(a)(1)(A), 1804(a)(4)(B), 1805(a)(3)(B), (c)(1)(B), (c)(3) (d). It is also used in Section 2.5 of Executive Order 12333.

[201] Indeed, Subsection (1) of the current definition was added after the other subsections had been established, in what appears to have been (in part, but not in whole) a belt-and-suspenders approach to regulating targeted surveillance of U.S. persons in the United States. See FISA Senate Judiciary Report at 32.

[202] Operation Shamrock was perhaps the government's largest electronic surveillance program (prior to September 11, 2001, in any event), and was conducted by the NSA or its predecessor organizations. For nearly thirty years, from 1945 to 1975, the NSA "received from international cable companies millions of cables which had been sent by American citizens in the reasonable expectation that they would be kept private." Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Report No. 94-755, Book II at 12 (1976) [hereinafter Church Report]. As the Church Committee Report explains:

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

Church Report Book III at 765 (footnote omitted). I do not mean to sensationalize by this reference to Operation Shamrock; nor is my point dependent on the technical aspects of Shamrock itself. The point is only that, if the government believes that the "particular, known" language in proposed Subsection (1) excludes (some forms of) driftnet surveillance, it could have far-reaching consequences, in part because of changes to the other subsections of the definition that are made by the government's proposal. It would be wise to resolve this issue in an authoritative fashion before changing the law.

[203] Current Subsection (2) does not use this language; it applies only when no party to the communication has consented to the surveillance.

[204] See FISA House Report at 54.

[205] Subsection (2) of the government's proposal refers to a "sender" and "recipients." Although these terms are most comfortably applied to electronic mail messages, FISA has always used them to refer to other forms of communication as well (see, e.g., Subsections (1) and (3) of the current definition), and Subsection (2) of the government's proposal by its terms applies to "any communication."

[206] This assumption is explored at length in the discussion of current FISA, above.

[207] Cf. *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc).

[208] 18 U.S.C. § 2511(1).

[209] 18 U.S.C. § 2511(1)(a) (emphasis added).

[210] 18 U.S.C. § 2511(1)(c) (emphasis added).

[211] 18 U.S.C. § 2511(1)(d) (emphasis added). There are other prohibitions in Title III, see 18 U.S.C. § 2511(1)(b) and (e), but the three provisions quoted in the text are the main ones.

[212] See 18 U.S.C. § 2510.

[213] 50 U.S.C. § 1801(f).

[214] 18 U.S.C. § 2511(2)(e). The terms "officer, employee, or agent" appear to cover everyone within the federal government who might be involved in a FISA surveillance, as well as some non-government personnel, and the requirement that the surveillance be conducted "in the normal course of ... official duty" likely does not significantly restrict the scope of the carve-out. See also 18 U.S.C. § 2511(2)(a)(ii) (authorizing specified third parties to assist the government in carrying out authorized FISA surveillance). These provisions were added to Title III by FISA as "conforming amendments necessary to integrate the Foreign Intelligence Surveillance Act into the existing provisions of [Title III]." FISA House Report at 98. In any event, current FISA itself provides that the FISC may issue an order authorizing surveillance under FISA, and that the Attorney General may authorize surveillance under 50 U.S.C. § 1802, "notwithstanding any other law," which probably is sufficient to insulate FISA surveillance from all other statutory limits. 50 U.S.C. § 1802(a)(1) & (b).

[215] Under 18 U.S.C. § 2511(2)(f), "[n]othing 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."

[216] 50 U.S.C. § 1802(a)(1) (electronic surveillance); see 50 U.S.C. § 1822(a)(1) (nearly identical provision for physical searches). The President authorized the Attorney General to exercise authority under these provisions in Section 1-101 of Executive Order 12139 (for electronic surveillance), and Section 1 of Executive Order 12949 (for physical searches).

[217] 50 U.S.C. §§ 1802(a)(3) (electronic surveillance) & 1822(a)(3) (physical search). FISA also provides that such certifications for electronic surveillance shall be retained by the FISC for "at least ten years." 50 U.S.C. § 1805(h). There is no corresponding provision for physical searches. Cf. 50 U.S.C. § 1824(f). The certification remains under seal unless the government applies for a court order on the ground that, despite expectations, the surveillance or search acquires the communication of, or involves the property of, a U.S. person. See 50 U.S.C. § 1802(a)(3) (electronic surveillance); 50 U.S.C. § 1822(a)(3) (physical search).

[218] 50 U.S.C. § 1802(a)(4) (electronic surveillance); 50 U.S.C. § 1822(a)(4) (physical search). Section 1802 does not expressly authorize physical entry into a foreign power's premises to conduct electronic surveillance, but in 1981 the

Department of Justice reversed its earlier interpretation of the statute and concluded that physical entry was implicitly authorized. See S. Rep. No. 98-660, at 6 (1984) [hereinafter Senate FISA Five Year Report].

[219] FISA House Report at 68.

[220] *Id.*

[221] *Id.*

[222] 50 U.S.C. § 1802(a)(1)(A)(1).

[223] 50 U.S.C. § 1802(a)(1)(A)(2).

[224] 50 U.S.C. § 1822(a)(1)(A)(i).

[225] 50 U.S.C. § 1802(a)(1)(A) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(i) (physical search).

[226] See FISA House Report at 29.

[227] *Id.*

[228] Section 1802 refers to "a foreign power" in the singular, while Section 1822 refers to "a foreign power or powers." Nonetheless, Section 1802 is best read to permit surveillance against property controlled exclusively by multiple foreign powers.

[229] Section 1822 authorizes the Attorney General to compel assistance from a "landlord" as well as other persons, strongly suggesting that rental property can fit within its scope. 50 U.S.C. § 1822(a)(4)(A). Thus, despite a landlord's ownership interest, leased property presumably could either be "used exclusively" by or be "under the open and exclusive control" of a foreign power tenant.

[230] FISA House Report at 70. The discussion in the legislative history actually concerns 50 U.S.C. § 1802(b), which is the provision governing ordinary FISA applications. But the phrase "notwithstanding any other law" also appears in 50 U.S.C. § 1802(a).

[231] Vienna Convention on Diplomatic Relations, Article 22, 23 U.S.T. 3227 (Apr. 18, 1961). See also id. at Article 24 ("The archives and documents of the mission shall be inviolable at any time and wherever they may be."); id. at Article 27 ("The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions ... The diplomatic bag shall not be opened or detained.").

[232] The 1978 legislative history also explains that the phrase "notwithstanding any other law" is meant to overcome any claim that, under 28 U.S.C. § 1251, the FISC cannot approve "surveillance directed at a foreign ambassador." FISA House Report at 70. Section 1802 does not apply where the surveillance is directed at "an agent of a foreign power, rather than at the foreign power itself." H.R. Conf. Rep. No. 95-1720 at 25 (1978).

[233] See Domestic Security Enhancement Act of 2003, Section-by-Section Analysis (Jan. 9, 2003) (available at www.pbs.org/now/politics/patriot2-hi.pdf).

[234] FISA House Report at 69.

[235] 50 U.S.C. § 1802(a)(1)(B) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(ii) (physical search).

[236] 50 U.S.C. § 1802(a)(1), (a)(1)(B) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A), (a)(1)(A)(ii) (physical search).

[237] 50 U.S.C. § 1801(a)(2); see FISA House Report at 29.

[238] 50 U.S.C. § 1801(a)(2); see FISA House Report at 29 ("The word 'substantially' means a significant proportion, but it may be less than a majority.").

[239] 50 U.S.C. §§ 1802(a)(1)(C) & (a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(iii) & (a)(1)(B) & (a)(2) (physical search). The Attorney General must also assess compliance with the minimization procedures and report to the Intelligence Committees as part of his semi-annual reporting obligations. 50 U.S.C. § 1802(a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(2) (physical search). (There is a mistaken cross-reference in the physical search provisions of FISA. Section 1822(a)(1)(A)(iii) refers to minimization procedures "under paragraphs (1) through (4) of Section 1821(4) of this title," when minimization procedures are in fact set out in paragraphs (A) through (D) of Section 1821(4).)

[240] 50 U.S.C. § 1802(a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(2)(physical search). See 50 U.S.C. § 1808(a) (semi-annual report on electronic surveillance); 50 U.S.C. § 1826 (same for physical searches).

[241] 50 U.S.C. § 1801(h)(4) (electronic surveillance); 50 U.S.C. § 1821(4)(D) (physical search). This requirement is contained in the statutory definition of "minimization procedures."

[242] In 2003, the Department of Justice wrote in a draft summary of proposed legislation that "[i]n essence, § 1802 authorizes the surveillance of communications between foreign governments, and between a foreign government and its embassy." See Domestic Security Enhancement Act of 2003, Section-by-Section Analysis (Jan. 9, 2003) (available at www.pbs.org/now/politics/patriot2-hi.pdf).

[243] I suspect the government did not intend this, but it is at least a plausible reading, and perhaps the best reading, of the introductory clause of proposed Section 1802A(a) and proposed Section 1802A(a)(3).

[244] See *United States v. Bin Laden*, 126 F. Supp. 2d 264 (SDNY 2000); see also *United States v. Marzook*, 435 F.Supp. 2d 778 (N.D. Ill. 2006).

[245] The Department of Justice has revealed that some FISA applications are "made solely for electronic surveillance, [some] applications [are] made solely for physical search, and [some are] combined applications requesting authority for electronic surveillance and physical search simultaneously." Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, to L. Ralph Meacham, Director, Administrative Office of the United States Courts (Apr. 30, 2004) (available at www.fas.org/irp/agency/doj/fisa/2003rept.pdf).

[246] 50 U.S.C. §§ 1801(g), 1804, 1823. DOJ has not publicly disclosed whether the Assistant Attorney General has been designated to approve FISA applications.

[247] OIPR is part of the DOJ National Security Division. See 72 Fed. Reg. 10064-01 (Mar. 7, 2007).

[248] FISA's legislative history explains that an application may be filed by "an attorney in the Department of Justice who ha[s] not personally gathered the information contained in the application," and that in such a case "it would be necessary that the application also contain an affidavit by an officer personally attesting to the status and reliability of any informants or other covert sources of information." FISA House Report at 73; *see* S. Rep. No. 103-296, at 60 (1994) [hereinafter FISA Search Senate Report]. The Department of Justice has confirmed publicly that attorneys in OIPR "prepare[] and file[] all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978," *see* U.S. Dep't of Justice, *Webpage of the Office of Intelligence Policy and Review*, *at* www.usdoj.gov/oipr, and that "OIPR does not conduct investigations," *see* U.S. Dep't of Justice, *Webpage of the Office of Intelligence Policy and Review*, *at* www.usdoj.gov/oipr/fisars.htm. Thus, some other entity, such as the FBI, must investigate, develop, and swear to the facts necessary to support a FISA application. In a speech given at the University of Texas on April 13, 2002, the then-Presiding Judge of the FISC, Royce Lamberth, explained that after reviewing the government's written submissions, "we then have the investigative agent appear before us, under oath, for questioning .... I do ask questions. I get into the nitty-gritty. I know exactly what is going to be done and why. And my questions are answered, in every case, before I approve an application. I know the

same is true of each of my colleagues." Judge Royce Lamberth, The Role of the Judiciary in the War on Terrorism (Apr. 13, 2002) (available at www.pbs.org/wgbh/pages/frontline/shows/sleeper/tools/lamberth.html).

[249] 50 U.S.C. § 1804(a)(1) (electronic surveillance); 50 U.S.C. § 1823(a)(1) (physical search). FISA's legislative history states that the applicant should be "the person who actually presents the application to the judge." FISA House Report at 73. That person is an OIPR (NSD) attorney. To approve the application, a judge of the FISC must find that "the application has been made by a Federal officer." 50 U.S.C. § 1805(a)(2) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search).

[250] In 2006, the word "specific" was added to 50 U.S.C. § 1804(a)(3), which governs electronic surveillance, out of concerns about roving surveillance. See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). The word does not appear in the corresponding provision for physical searches, 50 U.S.C. § 1823(a)(3). Orders approving FISA electronic surveillance and physical search applications must specify "the identity, if known, or a description of the [specific] target" of the search or surveillance, again with the word "specific" appearing only in the provision for electronic surveillance orders, 50 U.S.C. § 1805(c)(1)(A), not in the provision for physical search orders, 50 U.S.C. § 1824(c)(1)(A). The provision for electronic surveillance orders makes clear that the FISC's order must specify the identity or a description of the specific target "identified or described in the application." 50 U.S.C. § 1805(c)(1)(A).

[251] As noted earlier, the electronic surveillance provisions of FISA, enacted in 1978, refer to "his belief." 50 U.S.C. § 1804(a)(4). The physical search provisions, enacted in 1994, are gender neutral and refer to "the applicant's belief." 50 U.S.C. § 1823(a)(4).

[252] 50 U.S.C. § 1804(a)(4)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(4)(A) (physical search). Correspondingly, to approve the FISA application, the FISC must find probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3)(A) (electronic surveillance); 50 U.S.C. § 1824(a)(3)(A) (physical search).

[253] 50 U.S.C. § 1804(a)(4)(B). Correspondingly, to approve the FISA electronic surveillance application, the FISC must find probable cause that "each of the facilities or places" to be surveilled "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). The FISC's order must also specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." 50 U.S.C. § 1805(c)(1)(B).

[254] Although the application must state that the premises to be physically searched "contains" foreign intelligence information, 50 U.S.C. § 1823(a)(4)(B), there is no requirement of a corresponding specification in a FISC order authorizing a physical search. Nonetheless, this requirement in the application makes the physical search nexus requirements of FISA more like their traditional criminal counterparts.

[255] 50 U.S.C. § 1823(a)(4)(C). Correspondingly, to approve the FISA application, a FISC judge must find probable cause that the premises or property to be searched is "owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power." 50 U.S.C. § 1824(a)(3)(B). Although this provision differs from its counterpart for electronic surveillance in referring to property "used" rather than "used or about to be used" by a foreign power or an agent of a foreign power, *cf.* 50 U.S.C. § 1804(a)(4)(B), the other language in the provision probably makes up for any shortfall. Orders approving FISA physical search applications must also specify "the nature and location of each of the premises or property to be searched." 50 U.S.C. § 1824(c)(1)(B).

[256] 50 U.S.C. § 1804(a)(6). Correspondingly, orders approving FISA applications for electronic surveillance must specify "the type of communications or activities to be subjected to the surveillance." 50 U.S.C. § 1805(c)(1)(C).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. § 1801(a)(1)-(3) – a foreign government or component, a faction of foreign nations not substantially comprised of U.S. persons, or an entity openly acknowledged to be directed and controlled by a foreign government – and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the

application and order need not specify the type of communications or activities to be subjected to the surveillance. 50 U.S.C. §§ 1804(b), 1805(d). There is no corresponding provision for omitting this description or specification in physical search cases. Section 404 of the government's proposal would eliminate this distinction for official foreign powers.

[257] 50 U.S.C. § 1823(a)(3). This requirement of FISA physical search applications has no corresponding element in the required specifications of a FISC order authorizing a physical search, but orders approving FISA physical search applications must also specify the "type of information, material, or property to be seized, altered, or reproduced." 50 U.S.C. § 1824(c)(1)(C). According to the legislative history, the additional requirement for a "detailed description" in search applications is imposed so that the FISC may "meaningfully assess the sufficiency and appropriateness of the minimization procedures." FISA Search Senate Report at 62.

[258] 50 U.S.C. § 1804(a)(6) (electronic surveillance); 50 U.S.C. § 1823(a)(6) (physical search). Correspondingly, orders approving FISA applications must specify "the type of information" being sought. 50 U.S.C. § 1805(c)(1)(C) (electronic surveillance); 50 U.S.C. § 1824(c)(1)(C) (physical search). The certification that is part of every FISA application for electronic surveillance or a physical search also addresses this.

The precise statutory language governing electronic surveillance applications is "a detailed description of the nature of the information sought," 50 U.S.C. § 1804(a)(6); the precise language governing physical search applications is "a statement of the nature of the foreign intelligence sought," 50 U.S.C. § 1823(a)(6). The legislative history suggests that the two standards are not vastly different. The House Intelligence Committee report on the 1978 statute explains that "[t]he description should be as detailed as possible and sufficiently detailed so as to state clearly what sorts of information the Government seeks. A simple designation of which subdefinition of 'foreign intelligence information' is involved will not suffice." FISA House Report. The Senate Intelligence Committee report on FISA's 1994 physical search provisions states that the "statement should be sufficiently detailed so as to state clearly what foreign intelligence the Government seeks. A simple assertion that 'foreign intelligence information' is sought will not suffice. There must be an explanation of what specific foreign intelligence is sought." FISA Search Senate Report at 62.

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not include this information, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[259] 50 U.S.C. § 1804(a)(5) (electronic surveillance); 50 U.S.C. § 1823(a)(5) (physical search). Correspondingly, to approve a FISA application, the FISC must find that the minimization procedures proposed in the application meet the statutory definition of such procedures, which is set out at 50 U.S.C. §§ 1801(h) and 1821(4). 50 U.S.C. § 1805(a)(4) (electronic surveillance); 50 U.S.C. § 1824(a)(4) (physical search). Orders approving FISA applications must direct that the minimization procedures be followed. 50 U.S.C. § 1805(c)(2)(A) (electronic surveillance); 50 U.S.C. § 1824(c)(2)(A) (physical search).

[260] 50 U.S.C. § 1804(a)(8). Correspondingly, orders approving FISA applications for electronic surveillance must specify "the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance." 50 U.S.C. § 1805(c)(1)(D). Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. § 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not include this information, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[261] 50 U.S.C. § 1823(a)(6). Correspondingly, orders approving FISA applications for physical searches must specify "the manner in which the physical search is to be conducted." 50 U.S.C. § 1824(c)(1)(D). Moreover, although there is no corresponding requirement for physical search applications, "whenever more than one physical search is authorized," the FISC's order must specify "the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search." *Id.* The use of the words "a statement" in this provision is odd; typically, that phrase is used in FISA to describe the contents of an application, not the specifications of an

order. It may be that the asymmetry between physical search applications and orders was unintentional and that Section 1824(c)(1)(D) was originally drafted for inclusion in Section 1823.

[262] 50 U.S.C. § 1824(c)(2)(E); see Foreign Intelligence Surveillance Court Rule 16. There is no corresponding provision in electronic surveillance cases, but the FISC enjoys the power in both electronic surveillance and physical search cases to "assess compliance with the minimization procedures by reviewing the circumstances under which" information concerning U.S. persons was obtained pursuant to the surveillance or search. 50 U.S.C. § 1805(e)(3) (electronic surveillance); 50 U.S.C. § 1824(d)(3) (physical search).

[263] 50 U.S.C. § 1804(a)(9) (electronic surveillance); 50 U.S.C. § 1823(a)(9) (physical search). The two provisions are worded identically, except that the search provision refers to "persons, premises, or property," while the surveillance provision refers to "persons, facilities, or places."

[264] 50 U.S.C. § 1804(a)(10). Orders approving FISA applications for electronic surveillance must specify the "period of time during which the electronic surveillance is approved." 50 U.S.C. § 1805(c)(1)(E).

[265] 50 U.S.C. § 1804(a)(11). Correspondingly, when more than one electronic, mechanical, or other surveillance device is to be used, orders approving FISA applications for electronic surveillance must specify "the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device." 50 U.S.C. § 1805(c)(1)(F). Although FISA applications for physical searches need not contain any analogous statement, physical search orders must include "a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search." 50 U.S.C. § 1824(c)(1)(D).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, an application for electronic surveillance need not include this information describing the coverage of individual surveillance devices, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[266] Memorandum from FBI Headquarters, Office of the General Counsel, National Security Law Unit, to all FBI Field Offices, at 1-2 (April 5, 2001) [hereinafter "Woods Procedures"] (available at www.fas.org/irp/agency/doj/fisa/woods.pdf).

[267] The FISC's rules now explicitly permit electronic signatures on documents.

[268] Woods Procedures at 2. The demise of the FISA "wall" and old FISC Rule 11 presumably means that declarations no longer need report as much detail about related criminal investigations or prosecutions.

[269] *Id.*

[270] *Id.* at 2-11.

[271] The Woods Procedures were a response to a series of inaccuracies discovered in two unrelated sets of FISA applications submitted to the FISC in 2000 and 2001. For a more complete discussion of these inaccuracies and the government's response to them, see *In re all Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 611 (FISC 2002), rev'd, *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), and Testimony of David S. Kris before the Senate Judiciary Committee (Sept. 10, 2002) (available at www.usdoj.gov/dag/testimony/2002/krissenjud091002.htm).

[272] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search). To approve the FISA application, a FISC judge must find that the application "contains all statements and certifications required" by the statute, and "if the target is a United States person, the certification or certifications are not clearly erroneous." 50 U.S.C. § 1805(a)(5) (electronic surveillance); 50 U.S.C. § 1824(a)(5) (physical search).

[273] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search); *see* 50 U.S.C. § 402; Executive Order 12333 § 1.3(b).

[274] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search). The two certification provisions are identical except that the physical search provision contains a comma after "President" and provides that the certifying official must be appointed "by and with" rather than merely "with" the advice and consent of the Senate. Any reason for this different phrasing is lost in the historical mist. The certifying officials are designated in Executive Orders 12139 (for electronic surveillance), and 12949 (for physical searches). Both orders were amended in July 2005 by Executive Order 13383, in light of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004). The designated officials (in both amended orders) are: (a) Secretary of State; (b) Secretary of Defense; (c) Director of National Intelligence; (d) Director of the Federal Bureau of Investigation; (e) Deputy Secretary of State; (f) Deputy Secretary of Defense; (g) Director of the Central Intelligence Agency; and (h) Principal Deputy Director for National Intelligence. Under both executive orders, "[n]one of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate."

[275] *See In re* Sealed Case, 310 F.3d 717, 736 (FISCR 2002).

[276] *See* National Security Agency, *Presentation to the House Permanent Select Committee on Intelligence* (2000) (available at www.nsa.gov/releases/HPSCI_04122000/index.htm).

[277] 50 U.S.C. § 1804(a)(7)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(A) (physical search). "Foreign intelligence information" is defined at 50 U.S.C. § 1801(e) (and this definition is incorporated in FISA's physical search provisions, 50 U.S.C. § 1821(1)).

[278] 50 U.S.C. § 1804(a)(7)(B) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(B) (physical search). Prior to the Patriot Act, this provision required certification that "the purpose" of the search or surveillance was to obtain foreign intelligence information; courts interpreted that provision to require that the "primary purpose" be to obtain foreign intelligence information.

[279] 50 U.S.C. § 1804(a)(7)(C) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(C) (physical search).

[280] 50 U.S.C. § 1804(a)(7)(D) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(D) (physical search).

[281] 50 U.S.C. §§ 1804(a)(7)(E)(i)-(ii) (electronic surveillance); 50 U.S.C. §§ 1823(a)(7)(E)(i)-(ii) (physical search). Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the certification need not include this information. 50 U.S.C. § 1804(b). There is no corresponding provision allowing omission of this element of the certification in physical search cases.

[282] FISA House Report at 76 (referring to the certification as an "affidavit").

[283] *Id.* at 76; *see* FISA Search Senate Report at 62-63. The Foreign Intelligence Surveillance Court of Review has also emphasized the importance of the certification. *See In re* Sealed Case, 310 F.3d 717, 736 (FISCR 2002).

[284] 50 U.S.C. §§ 1804(d), 1805(a)(5) (electronic surveillance); 50 U.S.C. §§ 1823(c), 1824(a)(5) (physical search); FISA House Report at 75.

[285] 50 U.S.C. § 1804(a)(2) (electronic surveillance); 50 U.S.C. § 1823(a)(2) (electronic surveillance). Correspondingly, to approve the FISA application, a FISC judge must find that the President has authorized the Attorney General to make the application. 50 U.S.C. § 1805(a)(1) (electronic surveillance); 50 U.S.C. § 1824(a)(1) (physical search). The President authorized the Attorney General to make FISA electronic surveillance applications in Executive Order No. 12139, and to make FISA physical search applications in Executive Order No. 12949. In addition, Executive Order 12333 provides that the "Attorney General hereby is delegated the power to approve the

use for intelligence purposes, *within the United States* or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes." Exec. Order No. 12333 § 2.5 (emphasis added). This language was originally included to permit the Attorney General to authorize domestic physical searches in foreign intelligence cases, before FISA was amended (in 1994) to authorize such searches, FISA Search Senate Report at 37, but it would probably also satisfy FISA's requirement for Presidential authorization in electronic surveillance cases.

[286] 50 U.S.C. § 1804(a) (electronic surveillance); 50 U.S.C. § 1823(a) (physical search). Correspondingly, to approve the FISA application, a FISC judge must find that the Attorney General (as defined in the statute) has approved the application for filing. 50 U.S.C. § 1805(a)(2) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search). There is no requirement in FISA that the President approve individual FISA applications, although Presidents have done so in at least some cases. *See* Exec. Order No. 12036 §§ 2-201& 2-204; FISA Search Senate Report at 32-33, 59.

[287] FISA House Report at 73; *see* FISA Search Senate Report at 60-61.

[288] 50 U.S.C. § 1804(c) (electronic surveillance); 50 U.S.C. § 1823(b) (physical search). Correspondingly, the FISC may require a FISA applicant to submit additional information "as may be necessary to make the determinations required" under the statute. 50 U.S.C. § 1804(d) (electronic surveillance); 50 U.S.C. § 1823(c) (physical search). See also Foreign Intelligence Surveillance Court R. 10(d).

[289] 50 U.S.C. §§ 1804(e), 1824(d).

[290] *Id.*

[291] *Id.*

[292] *Id.* These provisions were enacted as part of the Intelligence Authorization Act for Fiscal Year 2001. Pub. L. No. 106-567, § 602(a), 114 Stat. 2831 (Dec. 27, 2000). Senator Specter, a key sponsor of the legislation, explained his view that they were necessary in light of DOJ's handling of the investigation of Wen Ho Lee. Reviewing what he believed were errors in the initial DOJ decision not to seek a FISA authorization in that case, Senator Specter went on to explain what (in his view) happened next:

> When [an] FBI Assistant Director ... raised the FISA problem with the Attorney General on August 20, 1997, she delegated a review of the matter to [an Associate Deputy Attorney General, or ADAG], who had virtually no experience in FISA issues. It is not surprising then, that [the ADAG] again applied the wrong standard for probable cause. He used the criminal standard, which requires that the facility in question be used in the commission of an offense, and with which he was more familiar, rather than the relevant FISA standard which simply requires that the facility "is being used, or is about to be used, by a foreign power or an agent of a foreign power."

146 CONG. REC. S9685-01 (daily ed. Oct. 3, 2000). Senator Specter's account is substantially similar to, and may be drawn from, the account set forth in the *Final Report of the Attorney General's Review Team (AGRT) on the Handling of the Los Alamos National Laboratory Investigation* ("[R]eview of the [FISA] application should not have been assigned to an Associate Deputy Attorney General who, despite his other considerable qualifications and expertise, had almost no prior experience with FISA applications .... The ADAG should have met with the FBI, and not just with OIPR, before determining that OIPR's evaluation of the application was correct .... The ADAG reached the wrong judgment .... The ADAG should have reported his findings to the Attorney General, who was never advised that the ADAG had decided the matter against the FBI.").

[293] The term "United States person" is defined in 50 U.S.C. § 1801(i) (and the definition is incorporated for physical search cases by 50 U.S.C. § 1821(1)).

[294] 50 U.S.C. § 1823(a)(8). The special concern about physical searches of U.S. persons' residences is understandable, but as a technical matter this is a curious provision because it overlaps substantially with the requirement of a certification (from a high-level, Senate-confirmed official) that the information being sought in the search "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1823(a)(7)(C). The certification must also contain "a statement explaining the basis" for that certification. 50 U.S.C. § 1823(a)(7)(E). The legislative history explains that the provision was added by the conference committee because of the "special concerns and sensitivities" involved in searching U.S. persons' residences and that the provision means to go beyond the certification requirement in the level of detail provided. FISA Search Conference Report at 58-59. By negative implication, however, it tends to suggest that certifications need not be very detailed. The conferees also apparently believed that requiring this statement from the Attorney General – rather than the certifying official – would further emphasize its importance.

[295] 50 U.S.C. § 1801(g). DOJ has not publicly revealed whether the Assistant Attorney General has been designated to approve FISA applications.

[296] 50 U.S.C. § 1804(a)(11).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, an application for electronic surveillance need not include this information describing the coverage of individual surveillance devices, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[297] 50 U.S.C. § 1804(a)(2).

[298] See 18 U.S.C. § 921(4)(B) (referring to a weapon "which has a barrel with a bore of more than one-half inch in diameter").