Modernizing the Foreign Intelligence Surveillance Act

A Working Paper of the Series on Counterterrorism and American Statutory Law, a joint project of the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution

By David S. Kris[*]

[*] David Kris is a graduate of Haverford College and Harvard Law School. After clerking for Judge Stephen S. Trott of the Ninth Circuit, he joined the Department of Justice through its Honors Program. He worked as a prosecutor for eight years, from 1992 to 2000, conducting several trials and arguing appeals across the country. From 2000 to 2003, he was Associate Deputy Attorney General. In that role, his unclassified responsibilities included supervising the government's use of the Foreign Intelligence Surveillance Act (FISA); representing the Justice Department at the National Security Council and in other inter-agency settings; briefing and testifying before Congress; and assisting the Attorney General in conducting oversight of the U.S. Intelligence Community. Mr. Kris received numerous awards at the Department of Justice, including the Attorney General's Award for Exceptional Service from Attorney General Janet Reno and from Attorney General John Ashcroft. Since 2003, he has been employed in the private sector, and continues to write, teach, and speak about national security law. He is the co-author, with Doug Wilson, of *National Security Investigations and Prosecutions* (West 2007).

Editor's Note

This paper is the first in a planned paper series on reforms to the statutory architecture of American counterterrorism policy, to be published jointly by the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution. The series is intended to suggest changes to areas of American statutory law pertinent to the War on Terrorism. Because of its obvious importance to an ongoing public policy debate, we are releasing Mr. Kris's paper as a working document that may undergo changes as the debate evolves over the coming months. Because of Mr. Kris's access while in government to classified material concerning national security surveillance programs, this paper required review for classified information and was approved for publication by the Department of Justice (DOJ) under 28 C.F.R. § 17.18.

Benjamin Wittes
Fellow and Research Director in Public Law
The Brookings Institution

Introduction

In December 2005, the New York Times reported,[1] and President Bush confirmed,[2] that the National Security Agency (NSA) had been conducting electronic surveillance of international communications, to or from the United States, without obeying the Foreign Intelligence Surveillance Act of 1978 (FISA).[3] The disclosure ignited a wildfire of political and legal controversy, which continues to generate heat, if not light, today.

Almost immediately after the surveillance was revealed, Congress responded in its oversight and lawmaking capacities, demanding information from the executive branch, and holding hearings on several bills.[4] The Bush Administration used those hearings to make the case for "FISA modernization" – statutory amendments that would, at a minimum, change the law to authorize explicitly what NSA had been doing since the fall of 2001. The government's central claim was that 30 years of technological change had artificially enlarged FISA's scope; the amendments it proposed were designed to restore the statute's original balance.

The policy questions began to crystallize in spring 2007, when the Bush Administration proposed a comprehensive set of legislative amendments, known as the FISA Modernization Act, and the Senate Intelligence Committee held an open hearing on the proposal.[5] That summer, with the Modernization Act still pending in Congress, the Administration made a hard push for a more limited set of changes to FISA, which became law in August 2007 as the Protect America Act (PAA).[6]

---

[1] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, New York Times at 1 (Dec. 16, 2005).

[2] See President's Radio Address (Dec. 17, 2005) (available at http://www.whitehouse.gov/news/releases/2005/12/20051217.html). The President stated: "I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks." For an explanation of why the President's program violated FISA, see *NSIP* Chapter 15.

[3] 50 U.S.C. §§ 1801 et seq.

[4] See, *e.g.*, Wartime Executive Power and the NSA's Surveillance Authority (Senate Judiciary Committee, Jan. 1, 2006) (available at http://judiciary.senate.gov/hearing.cfm?id=1727); Wartime Executive Power and the NSA's Surveillance Authority II (Senate Judiciary Committee, Feb. 28, 2006) (available at http://judiciary.senate.gov/hearing.cfm?id=1770); NSA III: Wartime Executive Powers and the FISA Court (Senate Judiciary Committee, Mar. 28, 2006) (available at http://judiciary.senate.gov/hearing.cfm?id=1825); FISA for the 21st Century (Senate Judiciary Committee, July 26, 2006) (available at http://judiciary.senate.gov/hearing.cfm?id=698); Modernizing the Foreign Intelligence Surveillance Act (House Intelligence Committee, July 19, 2006 (available at http://intelligence.house.gov/EventsItem.aspx?id=213); Full Committee Meeting on FISA Legislation (House Intelligence Committee, July 27, 2006) (available at http://intelligence.house.gov/EventsItem.aspx?id=214).

[5] The text of the Administration's proposal, the testimony of witnesses, and statements submitted for the record are available on the website of the Senate Intelligence Committee (http://intelligence.senate.gov/hearings.cfm?hearingId=2643).

[6] Pub. L. No 110-55, 121 Stat. 52 (2007).

Although narrower than the Modernization Act, the PAA still made substantial changes to FISA. Where FISA previously regulated surveillance in the United States of wire communications into or out of this country, and surveillance of stored e-mail in this country (even if sent between persons located abroad),[7] the PAA provides that FISA does not apply to any surveillance "directed at a person reasonably believed to be located outside of the United States," regardless of where the surveillance occurs.[8] It was, and is, a very significant statute, albeit with a relatively short lifespan due to its sunset provision.[9]

Congress began considering replacements for the PAA almost immediately after it was enacted. By October 2007, the House of Representatives had drafted the Responsible Surveillance that is Overseen, Reviewed and Effective (RESTORE) Act,[10] and the Senate Intelligence Committee had approved the FISA Amendments Act of 2007 (FAA).[11] As of this writing, however, neither bill has reached the floor of either House of Congress.

This paper discusses the justification for, and the meaning of, the PAA, the RESTORE Act, and the FAA. Its principal conclusions may be summarized as follows:

First, the government's claim, in support of the PAA, that "almost all" transoceanic[12] communications were carried by satellite in 1978, appears to be exaggerated. The evidence reviewed in Part II of this paper indicates that between one-third and one-half of such communications were carried by undersea cable. The government may have evidence to support its claim, and I welcome correction at any time, but to date I have not seen anything to rebut my conclusions.

Second, as explained in Part III, Congress enacted FISA principally to regulate surveillance of domestic communications, and of international communications made by

---

[7] See *NSIP* Chapter 7.

[8] 50 U.S.C. § 1805A.

[9] PAA Section 6.

[10] H.R. 3773; see H.R. Rep. No. 110-373 (Oct. 12, 2007). The text of the RESTORE Act is available on the website of the Library of Congress, http://thomas.loc.gov/cgi-bin/query/D?c110:2:./temp/~c1109fA0b9.

[11] S. 2248; see S. Rep. No. 110-209 (Oct. 26, 2007). A draft of the FAA is available on the website of the Senate Select Committee on Intelligence, http://intelligence.senate.gov/071019/fisa.pdf.

[12] Unless otherwise indicated in context, this paper uses the following terms with the following meanings: (1)"Transoceanic" refers to a communication transmitted between locations separated by an ocean – *e.g.*, a telephone call from New York to London. A similar term is "intercontinental." (2) "International" refers to a communication transmitted between the United States and a foreign country – *e.g.*, a telephone call from New York to London, or a telephone call from Mexico City to New York. A similar term is "one-end-U.S." (3) "Foreign-to-foreign" refers to a communication transmitted between locations outside the United States – *e.g.*, a telephone call from Paris to London. (4) "Domestic" refers to a communication transmitted between locations inside the United States – *e.g.*, a telephone call from Washington, D.C. to New York.

targeting particular, known Americans located in the United States.[13] It understood that, as a legal matter, the NSA remained free after 1978 to continue "vacuum cleaner" acquisition of international communications – including communications to, from, or about Americans located in the United States – using any or all of three methods:

- radio surveillance of transmissions to or from satellites;
- wire surveillance of coaxial cables on Canadian or other foreign soil; or
- wire surveillance of coaxial cables in international waters.[14]

To be sure, FISA regulated wire surveillance of international communications on U.S. soil, but this may have been based on concerns that wires inside the United States also carried domestic communications. Congress intended subsequent legislation to fill the gaps left by FISA, but for a variety of reasons such legislation was never enacted.[15]

Third, while telecommunications history and legislative history are interesting and relevant, current policy makers should not be prisoners to the judgments of 1978. In my view, today's central operational problem is the difficulty of determining the location of parties to an electronic communication, largely because of changes in telecommunications technology and increased globalization. As explained in Part IV, this operational problem undermines FISA's reliance on geography to resolve what I believe is the central policy question presented today: when should the government be allowed to conduct foreign intelligence wiretaps without individualized warrants?[16] As I read the PAA, it answers this policy question in favor of warrantless surveillance in three areas:

- The PAA permits warrantless surveillance of foreign-to-foreign e-mail messages acquired from storage on servers located in the United States. This change enjoys broad political support, largely because FISA has never regulated surveillance of foreign-to-foreign telephone calls acquired from switches located in the United States.

---

[13] Unless otherwise indicated in context, this paper uses the term "American" to refer to "United States persons" as defined by FISA – e.g., American citizens and lawful permanent resident aliens. See 50 U.S.C. § 1801(i). For a more complete discussion of the term "United States person," see *NSIP* Chapter 8.

[14] In keeping with FISA's definitions, this paper uses "radio surveillance" to mean surveillance of a radio wave, and "wire surveillance" to mean surveillance of a wire, cable, or other like connection. 50 U.S.C. § 1801(*l*). This contrasts with the use of similar terms in other wiretapping laws. For a more complete discussion of this issue, see *NSIP* Chapter 7.

[15] See, *e.g.*, S. Rep. No. 95-701 at 35 (1978).

[16] See David Kris, Post # 3 in *What's the Big Secret*, Slate Magazine (Aug. 28, 2007) (available at http://www.slate.com/id/2172952/entry/2172969/) [hereinafter Slate Discussion]. This paper uses "warrantless" to refer to surveillance conducted without (advance) approval from the FISA Court, in contrast to surveillance conducted with judicial approval. (For a discussion of whether a FISA order is a genuine Fourth Amendment "Warrant," rather than a mere court "order" authorizing surveillance, see *NSIP* Chapter 11.) The paper refers to surveillance "exempted from FISA" or "outside the scope of FISA" to mean the same thing – i.e., surveillance that is not "electronic surveillance" as defined by FISA, 50 U.S.C. § 1801(f), and therefore exempt from FISA's general requirement that "electronic surveillance" be conducted pursuant to court order.

- The PAA permits warrantless surveillance of international communications to or from the United States, even when acquired from a wire (or an e-mail server) inside the United States. This change remains controversial because it makes FISA narrower in scope than it was in 1978.

- The PAA permits warrantless surveillance of domestic communications in certain circumstances. The government disputes this, but I respectfully disagree. The executive branch may decide as a prudential matter to eschew such surveillance, but absent further explanation from the Justice Department, I see nothing in the PAA to prevent it.

The RESTORE Act and the FAA, both pending in Congress at this writing, take the same basic approach as the PAA, albeit with additional procedural and substantive safeguards and limits. But they raise a number of policy and technical issues that should be considered before either bill becomes law. Those issues are discussed in general terms in Part V (and discussed in detail in an appendix). Part VI of the paper is a short conclusion.

I. BACKGROUND

As enacted in 1978, FISA essentially regulated and authorized electronic surveillance of foreign powers and agents of foreign powers in the United States. As explained elsewhere,[17] FISA has never applied to ordinary criminals, such as burglars and murderers, and its extremely complex definition of "electronic surveillance"[18] defines both the precise nature, and location, of the investigative activity that it governs.[19] The statute does not apply (and has never applied) where all parties to a wire or radio communication are located abroad, even if they are American citizens, and even if the communication is intercepted inside the United States. Nor has the statute ever regulated surveillance that is conducted abroad of a person who is located abroad, even if the person is an American.[20] However, until the PAA in August 2007, FISA did regulate wire surveillance in the United States of communications to or from a person in the United States, even if the person was a visiting foreigner; and it also regulated surveillance of stored e-mail in the United States, even if the e-mail was exchanged between two foreigners located abroad.[21]

[17] *NSIP* Chapters 5 and 8.

[18] 50 U.S.C. § 1801(f)(1)-(4), discussed in *NSIP* Chapter 7; see also 50 U.S.C. § 1805A.

[19] See *NSIP* Chapter 7.

[20] See *NSIP* Chapter 7. Surveillance abroad that is directed at a U.S. person who is located abroad is regulated by Section 2.5 of Executive Order 12333. See *NSIP* Chapter 16.

[21] This is because stored e-mail is neither a wire nor a radio communication under FISA. See *NSIP* Chapter 7.

Where FISA applies, it generally requires a court order before any surveillance may begin.[22] Obtaining such a court order takes time,[23] and requires the personal involvement and signature of at least two very senior national security officials.[24] In 1979, the first year after FISA's enactment, the government filed 199 applications; in 2006, the last year for which data is available, it filed 2,181 applications.[25] The government has complained that, in the post 9-11 era, FISA unduly restricts its "speed and agility."[26]

For present purposes, there are three essential elements of a FISA application and order for electronic surveillance.[27] First, the government must establish, and a judge of the FISA Court must find, probable cause that the "target" of the surveillance – the person or entity from or about whom the government seeks information – is a "foreign power," such as an international terrorist group, or an "agent of a foreign power," such as a member of an international terrorist group.[28] Second, there must also be probable cause that the target is using, or is about to use, the particular "facility," such as a telephone number or e-mail address, at which the surveillance will be

---

[22] There are four exceptions to this general requirement, as explained in *NSIP* Chapter 12. One exception is for emergency surveillance. See 50 U.S.C. § 1805(f). For a discussion of how this exception works in practice, see Frontline, Spying on the Home Front (interview with James Baker) (available at http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/baker.html).

[23] The Director of National Intelligence (DNI) recently asserted that it takes "200 man hours" to prepare a FISA application "for one [telephone] number." See Chris Roberts, Transcript: Debate on the Foreign Intelligence Surveillance Act, *El Paso Times* (Aug. 22, 2007) (available at http://www.elpasotimes.com/news/ci_6685679) [hereinafter El Paso Transcript].

[24] See *NSIP* Chapter 6.

[25] See *NSIP* Chapter 13.

[26] See, *e.g.*, CNN, *Administration Defends NSA Eavesdropping to Congress* (Dec. 23, 2005) (available at http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html). In defending the controversial Terrorist Surveillance Program (TSP) confirmed by the President in December 2005, the government has explained that the "President authorized the TSP because it offers … speed and agility …. Among the advantages offered by the TSP compared to FISA is *who* makes the probable cause determination and how many layers of review will occur *before* surveillance begins." Responses to Joint Questions from House Judiciary Committee Minority Members, Response to Question 32 (released Mar. 24, 2006) (italics in original) [hereinafter HJC Minority QFRs 3-24-06]. The government's explanation continues:

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

HJC Minority QFRs 3-24-06, Response to Question 32 (second alteration in original). In sum, the government reports, the "relevant distinction between the two methods – and the critical advantage offered by the TSP compared to FISA – is the greater speed and agility it offers." HJC Minority QFRs 3-24-06, Response to Question 34.

[27] For a more complete discussion of the required elements of a FISA application for electronic surveillance, see *NSIP* Chapter 6.

[28] For a discussion of the terms "target," "foreign power," and "agent of a foreign power," see *NSIP* Chapter 8. The term "target" is not defined in FISA, although legislative history explains its meaning; the terms "foreign power" and "agent of a foreign power" are defined in 50 U.S.C. § 1801.

directed.[29] Third, the government's application must propose, and the FISA Court's order must require adherence to, "minimization procedures." Essentially, these are specific procedures designed to balance the government's need to obtain intelligence against the privacy interests of Americans.[30] Thus, for example, if a terrorist were using a particular public telephone, the government might be authorized to tap the phone, but only when the terrorist was known to be using it, thus minimizing the acquisition of any calls made by other persons.[31]

II. TELECOMMUNICATIONS HISTORY

A. The Government's Claim.

The government argued in favor of the PAA on the ground that technological change had inadvertently expanded the scope of FISA. According to the government, nearly 30 years ago, when FISA became law, international telephone calls were "almost all" transmitted by means of radio waves that bounced off satellites orbiting the earth. Where it wished to eavesdrop on such calls made by visiting foreigners, NSA could do so by intercepting the radio waves. And it could do so without regard to FISA, which contained an exemption for international radio communications – as opposed to international wire communications – as long as the government was not seeking information from or about particular Americans located in the United States.[32]

In the years since 1978, however, the government claimed that communications satellites were replaced by undersea fiber optic cables, effectively reducing the use of radio waves to transmit international calls. This improved call quality, but also limited the government's authority, because FISA treats surveillance of a wire (or cable) differently than surveillance of a radio wave.[33] Thus, the argument went, the PAA was necessary to restore FISA's original balance.

This historical claim was advanced by many senior government officials. For example, General Michael Hayden, the Director of the CIA (and former Director of the NSA), testified before Congress that for "reasons that seemed sound at the time, the current statute makes a distinction between collection 'on a wire' and collection out of the air. When the law was passed, almost all local calls were on a wire and almost all long haul communications were in the air. In an age of cell phones and fiber optic cables, that has been reversed … with powerful and unintended consequences for how

[29] For a discussion of the term "facility," see *NSIP* Chapters 6 and 15. This term is not defined in FISA, although legislative history explains its meaning.

[30] For a discussion of "minimization" under FISA, see *NSIP* Chapter 9.

[31] In most FISA cases, recording devices are left on at all times, and minimization first occurs in the process of logging and indexing communications for future use, as explained in *NSIP* Chapter 9.

[32] See 50 U.S.C. § 1801(f)(1) and (3), discussed in *NSIP* Chapter 7.

[33] Compare 50 U.S.C. § 1801(f)(2), with 50 U.S.C. § 1801(f)(3). For a more complete discussion of this issue, see *NSIP* Chapter 7.

NSA can lawfully acquire a signal."[34] Similarly, the current Director of NSA, General Keith Alexander, wrote to Congress that "[w]hen FISA was enacted in 1978, almost all transoceanic communications into and out of the United States were carried by satellite," and therefore "intentionally omitted from the scope of FISA."[35] General Alexander went on to explain that the subsequent and unanticipated migration from satellite to fiber optic cable for overseas calling, "rather than a considered judgment by Congress, has resulted in the considerable expansion" of FISA's regulatory reach.[36] Echoing these sentiments nine months later, Kenneth Wainstein, the Justice Department's Assistant Attorney General for National Security, testified that in 1978, "almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as 'radio' (vs. 'wire') communications."[37] Finally, Admiral Mike McConnell, the Director of National Intelligence, testified that when FISA "was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as 'wireless' communications."[38] Today, he asserted, "the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air."[39]

Not everyone accepted the government's claim. For example, Kate Martin and Lisa Graves, the Director and Deputy Director of the Center for National Security Studies, wrote to Congress on May 1, 2007, that "even a general examination of telecommunications history … reveals that the scenario they posit is not accurate. While satellites were increasingly used in the 1970s … American telephone companies were continuing to rely on trans-oceanic cables for international calls, with newer transatlantic cables sunk even the year after FISA passed."[40] Congress did not make

---

[34] Testimony of General Michael V. Hayden, Director of Central Intelligence, before the Senate Committee on the Judiciary (July 26, 2006) (ellipsis in original) (available at http://judiciary.senate.gov/testimony.cfm?id=698&wit_id=5604) [hereinafter Hayden Testimony 7-26-06].

[35] Letter from Lt. Gen. Keith B. Alexander, Director, National Security Agency, to Senator Arlen Specter, Chairman, Committee on the Judiciary, United States Senate at 1 (Dec. 19, 2006) (answer to Question 2a for Senator Specter) (available at http://www.fas.org/irp/congress/2006_hr/alexander-qfr.pdf) [hereinafter Alexander QFRs 12-19-06].

[36] Alexander QFRs 12-19-06 (answer to Question 2a for Senator Specter).

[37] Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice, before the House Permanent Select Committee on Intelligence at 4 (Sept. 6, 2007) (available at http://www.usdoj.gov/nsd/docs/2007/wainstein-statement-9-6-07.pdf) [hereinafter Wainstein Testimony 9-6-07]. See also Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice, before the House Permanent Select Committee on Intelligence at 4 (Sept. 20, 2007) (same) (available at http://www.usdoj.gov/nsd/docs/2007/wainstein-HPSCI-statement-9-20-07.pdf) [hereinafter Wainstein Testimony 9-20-07].

[38] Statement of Director of National Intelligence Michael McConnell before the Senate Select Committee on Intelligence at 3 (May 1, 2007) (emphasis in original) (available at http://intelligence.senate.gov/070501/mcconnell.pdf) [hereinafter McConnell Testimony 5-1-07].

[39] McConnell Testimony 5-1-07 at 4.

[40] Statement of Kate Martin, Director, and Lisa Graves, Deputy Director, Center for National Security Studies, before the Senate Select Committee on Intelligence at 10 (May 1, 2007) (available at http://intelligence.senate.gov/070501/martingraves.pdf) [hereinafter Martin-Graves Statement 5-1-07].

any formal findings in conjunction with the PAA, but it appears to have accepted the essential accuracy of the government's narrative account, at least on a temporary basis.

B. The Historical Evidence.

The historical record that I have reviewed indicates that the government's claim is exaggerated: in and around 1978, transoceanic communications were made in relatively large quantities by both satellites (radio) and coaxial cables (wire); both kinds of systems were expected to continue in service for many years; and the use of fiber optics was already anticipated for undersea cables.[41] Of course, I am neither an historian nor a communications lawyer, and I welcome correction if there is evidence to the contrary, but so far I have seen none.

The first transatlantic communications cable was laid in 1858,[42] approximately mid-way between the inventions of the telegraph (1839) and the telephone (1876).[43] Although this cable failed very quickly, a new and more durable cable was laid in 1866.[44] This and other telegraph cables lacked the bandwidth to carry voice communications, however, and the first transatlantic telephone call was therefore made by conventional radio signal in 1915, the same year that transcontinental telephone service became available by wire within the United States.[45] Commercial transatlantic telephone service, still using radio, was initially offered between the U.S. and the U.K. in 1927 (one call at a time, and apparently at a rate of $75 for the first three minutes).[46] In the 1930s, coaxial cable came into use for telephone calls within the United States,[47] and microwave radio transmitters were first used domestically in the following decade.[48]

The first (relatively) high-capacity transatlantic cable became operational in 1956 (and remained in service until 1979, the year after FISA was enacted). This cable,

---

[41] For background on the international telecommunications industry in the late 1970s and early 1980s, see, *e.g.*, *ITT v. FCC*, 725 F.2d 732, 736-737 (D.C. Cir. 1984). For background on the Federal Communication Commission's (FCC's) licensing power for overseas communications, see *FCC v. RCA*, 346 U.S. 86 (1953). For an explanation of how international communications were transmitted from the United States via satellite earth stations and cable head ends located in gateway cities, see *Western Union v. FCC*, 568 F.2d 1012, 1014-1015 (2d Cir. 1977).

[42] Amos Joel, *Retrospective, Telecommunications and the IEEE Communications Society*, IEEE Communications Magazine, 50th Anniversary Commemorative Issue (May 2002) at 6 [hereinafter Retrospective].

[43] Retrospective at 6-7.

[44] Retrospective at 6.

[45] Bell Telephone, 100 Years of Service (available at www.porticus.org/bell/att/1975/1975_his.htm) [hereinafter 100 Years of Service]; see also Milestones in AT&T History (available at www.corp.att.com/history/milestones.html) [hereinafter Milestones]; Retrospective at 8-10.

[46] Milestones.

[47] 100 Years of Service.

[48] Retrospective at 10.

known as TAT-1, could carry 36 voice channels simultaneously.[49] A similar cable was laid across the Pacific Ocean, from California to Hawaii, the following year.[50] Over the next several years, additional coaxial cables were laid across both oceans, with larger capacities and longer lifespans.[51] In its 1975 annual report to shareholders, for example, AT&T proudly announced that TAT-6 would "carry 4,000 calls simultaneously. It has four times the capacity of the fifth transatlantic cable, laid in 1970, and … it is designed to operate trouble-free for at least 25 years."[52] The following year, AT&T made similar claims, reporting a "major advance in undersea cable technology."[53] In 1978 and 1979, the FCC approved plans for TAT-7,[54] and AT&T later announced to its shareholders that the cable was "expected to be in service in July, 1983."[55]

The first commercial communications satellite, Telstar I, was launched in 1961, and more durable satellites followed in 1963 and subsequent years.[56] By 1974, Intelsat could boast that its satellites carried "5,000 international telephone circuits," including both transatlantic and transpacific channels.[57] By 1975, there were three Intelsat IV satellites in orbit carrying transatlantic calls (and two carrying transpacific calls), each with a capacity of approximately 4,000 circuits.[58] These satellites could transmit overseas calls using microwave signals (and could also broadcast television signals).[59]

---

[49] Retrospective at 10; 100 Years of Service; see FCC, International Bureau, *Trends in the International Telecommunications Industry* 2 (Sept. 2005) [hereinafter FCC Trends Report 2005]; cf. FCC Trends Report 2005 at 9 (40 usable voice channels).

[50] IEEE, History of the Technology, Chapter 2: 1952-1964 [hereinafter History of the Technology]. Other transpacific cables included the COMPAC and ANZCAN cables. See, *e.g.*, *In re Inquiry into the Policies to be Followed in the Authorization of Common Carrier Facilities to Meet Pacific Telecommunications Needs During the Period 1981-1995*, 94 F.C.C.2d 867 (1983).

[51] Retrospective at 10. For a chart of the various TAT cables, including some of the more modern fiber optic cables, see Jim Lande and Linda Blake, Industry Analysis Division, Common Carrier Bureau, Federal Communications Commission, *Trends in the U.S. International Telecommunications Industry* at 25 (table 11) (June 1997) [hereinafter FCC Trends Report 1997].

[52] AT&T, 1975 Annual Report to Shareholders at 10 (available at www.porticus.org/bell/att/1975/att_1975.htm) [hereinafter AT&T 1975 Report]. Until the 1980s, AT&T had "a virtual monopoly on [international telephone] service from the U.S. mainland." FCC Trends Report 2005 at 6.

[53] AT&T, 1976 Annual Report to Shareholders at 9, 11 (available at www.porticus.org/bell/att/1976/att_1976.htm) [hereinafter AT&T 1976 Report].

[54] See 71 F.C.C.2d 64 (1979); 73 F.C.C. 2d 248 (1979).

[55] AT&T 1979 Annual Report to Shareholders at 8 (available at www.porticus.org/bell/att/1979/att_1979.htm) [hereinafter AT&T 1979 Report].

[56] Retrospective at 12.

[57] Intelsat, About Us, Our History (available at www.intelsat.com/about-us/history/intelsat-1970s.asp).

[58] Delbert Smith, *Communication via Satellite: A Vision in Retrospect* at 154 (1976); D.I. Dalgleish, *Introduction to Satellite Communications* at 14 (1989); cf. NASA, Image of the Day, In a Sound Chamber (Intelsat IV had a "capacity of about 6,000 circuits") (available at www.nasa.gov/multimedia/imagegallery/image_feature_527.html); Boeing, Intelsat IV (same) (available at http://www.boeing.com/defense-space/space/bss/factsheets/376/intelsat_iv/intelsat_iv.html). For details on the launch dates and deployment of the Intelsat IV, and other Intelsat satellites, see *In re Communications Satellite Corporation*, 56 F.C.C.2d 1101 (1975); see also, *e.g.*, *In re Comsat*, 32 F.C.C.2d 537 (1971) (authorizing Comsat to launch Intelsat IV (F-3) on or about September 17, 1971).

[59] Retrospective at 12.

By 1976, AT&T was preparing to launch three new communications satellites, explaining that "[s]atellites, along with undersea cables, have been used to provide overseas telephone service for the last 11 years," but that these three "will be our first use of satellite channels for domestic telephone calls."[60] Indeed, satellites were first used by AT&T for domestic communications later that year, having been "integrated with the microwave radio and coaxial cable circuits that make up the bulk of [AT&T's] interstate telecommunications network."[61] The company also noted in its 1976 report that improvements to its microwave capacities were "under development," and "could more than double the capacity of our existing microwave routes without large capital investment."[62]

The total volume of transoceanic calls rose steadily through the 1970s,[63] causing the FCC to "develop a comprehensive approach" designed to establish "a complete facilities-configuration proposal (i.e., cable and satellite facilities)" for transoceanic calls.[64] This resulted in a policy known as "balanced loading," under which "all growth

---

[60] AT&T 1975 Report at 10.

[61] AT&T 1976 Report at 11.

[62] AT&T 1976 Report at 12.

[63] In 1977, for example, AT&T reported that "overseas calling – 106 million messages – was up 23 percent." AT&T 1977 Annual Report to Shareholders at 14 (available at www.porticus.org/bell/att/1979/att_1979.htm) [hereinafter AT&T 1977 Report]. The following year overseas calling "continued to grow by about 27 percent." AT&T 1978 Annual Report to Shareholders at 5 (available at www.porticus.org/bell/att/1978/att_1978.htm) [hereinafter AT&T 1978 Report]. For current data on transoceanic circuits and calling, see FCC, International Bureau Report, 2005 Section 43.82 Circuit Status Data (Jan. 2007) (available at http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-269605A2.pdf), and FCC, International Bureau, 2005 International Telecommunications Data (Apr. 2007) (available at http://www.fcc.gov/ib/sand/mniab/traffic/files05/CREPOR05.pdf).

[64] *In re Inquiry into the Policies to be Followed in the Authorization of Common Carrier Facilities to Meet North Atlantic Telecommunications Needs During the 1985-1995 Period*, 82 F.C.C.2d 407 (1980) (discussing regulation of transatlantic communications during the 1970s). The FCC first began comprehensive regulation of transpacific calls in 1981. See *In re Inquiry into the Policies to be Followed in the Authorization of Common Carrier Facilities to Meet Pacific Telecommunications Needs During the Period 1981-1995*, 94 F.C.C.2d 867 (1983). At the same time, the FCC was regulating satellite communications using its authority under the Communications Satellite Act of 1962 in part to ensure the continued "significant investment in [transoceanic] cable facilities" by the telephone companies. *Proposed Modification of the Commission's Authorized User Policy Concerning Access to the International Satellite Services of the Communications Satellite Corporation*, 100 F.C.C.2d 177 (1985) [hereinafter *In re Comsat*]. By 1982, however, the FCC no longer felt the need to protect providers of transoceanic cables from competing satellite service being offered directly to individual users, and by 1984 it could not say "whether, in general, cable circuits are more costly than satellite circuits." *In re Comsat*, 100 F.C.C.2d 177 (discussing a 1980 published notice of proposed rulemaking, and a 1982 decision that was challenged in the D.C. Circuit but reaffirmed in 1984 and published in 1985).

During the 1970s, and thereafter, AT&T had an economic incentive to prefer transoceanic cable to satellite because it could earn a greater return from the former than the latter. See *In re Comsat*, 100 F.C.C.2d at n.37. This led to considerable argument before the FCC. For example, in 1977, the FCC concluded that "any plan which includes the construction of an additional North Atlantic cable facility during the 1977-1985 period would apparently impose a substantial and unnecessary cost burden on U.S. telecommunications entities and users," because "addition of the INTELSAT-V satellites now under construction, together with existing cable and satellite facilities, would provide sufficient capacity to handle [anticipated] traffic increases, with or without an additional cable facility." *In re Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, 67 F.C.C.2d 358 (1977). Based on motions for reconsideration from the telephone companies, and from the U.S. Department of Defense, the FCC later relented, allowing TAT-7 to be built. See *In re AT&T*, 73 F.C.C.2d 248 (1979) (recounting the history of this period).

circuits are assigned to a new facility upon its introduction until its load level equals existing routes."[65] As part of balanced loading efforts, the FCC in 1977 authorized AT&T to activate additional circuits on the TAT-6 transatlantic cable, over the objections of Comsat (the Communications Satellite Corporation), "so that a reasonable number of circuits will be maintained in each route to provide adequate diversity" between cables and satellites.[66] During the course of the 1970s, satellites carried a significant – and increasing – percentage of transoceanic calls.[67] But even well after FISA's enactment, at the end of the 1970s, when one source reports that "more than two thirds of all international telephony was routed through satellite channels,"[68] millions and millions of calls still crossed the oceans on underwater cables.

Moreover, even as satellite use was increasing, fiber optic cable was already on the horizon.[69] Based on test deployments in Atlanta, Georgia, AT&T predicted in its 1975 report that fiber optics could be in use "perhaps in the early 1980s."[70] The following year, the company announced that results of testing "exceeded our expectations and pointed to an early application of this new communications technology."[71] By the 1978 report, fiber optic cable had come "through a year-long service test in Chicago with flying colors," and was to be installed "in the Atlanta metropolitan area linking two central offices and a long distance switching center."[72] The company also announced in that report that fiber optics were "expected to be used for local lines, long distance routes and undersea cable."[73]

In short, at the time Congress was considering and enacting FISA, from 1974 to 1978, it does not appear to be the case that "almost all" overseas calls were carried on satellites; the actual portion was probably somewhere between one-half and two-thirds.[74] Indeed, the Defense Department (NSA's parent agency) had a policy in 1979

---

[65] *In re Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, 71 F.C.C.2d 71 (1979).

[66] *In re AT&T*, 63 F.C.C.2d 166 n.7 (1977).

[67] In November 1971, AT&T was providing 703 cable, 631 satellite, and 13 high-frequency radio telephone circuits between the United States and Europe, and was anticipating rough parity between cable and satellite circuits through 1980. *In re AT&T, ITT, RCA, and Western Union*, 35 F.C.C.2d 801 (1972). In 1974, the FCC allowed AT&T to "maintain, until mid-1976, a 1 to 1 satellite to cable circuit ratio to countries accessing only one Atlantic satellite or a 2 to 1 satellite to cable ratio to countries accessing both Atlantic satellites." *In re AT&T*, 52 F.C.C.2d 128 (1975) (describing 1974 decision).

[68] Satellite Communication, Encyclopedia Britannica (2007) (available at www.britannica.com/eb/article-224536).

[69] AT&T 1975 Report at 10.

[70] AT&T 1975 Report at 21.

[71] AT&T 1976 Report at 12.

[72] AT&T 1978 Report at 7.

[73] AT&T 1978 Report at 7. By 1980, the FCC was already reviewing plans for undersea fiber optic cables. *In re Inquiry into the Policies to be Followed in the Authorization of Common Carrier Facilities to Meet North Atlantic Telecommunications Needs During the 1985-1995 Period*, 82 F.C.C.2d 407 (1980).

[74] In 1985, AT&T appears to have proposed "to move from a 52 percent satellite/48 percent cable use ratio which will obtain at year end 1985 under balanced loading to a ratio of 40 percent satellite/60 percent cable by year-end 1989." *In re Inquiry into the*

of "placing one-third of its overseas communications requirements on each of commercial cable, commercial satellites, and military satellites."[75] Thus, as AT&T explained to its shareholders in early 1980, the "nationwide telecommunications network … connects some 175 million telephones via a complex web of 1.4 billion miles of microwave and cable paths and 12,000 satellite circuits. And it is linked to the rest of the world's telephones by undersea cable and satellite."[76] The company was relying on both "higher capacity cable system[s]" and "increased use of overseas satellite circuits" to "keep pace with the rapidly growing volume of international calling,"[77] and it was looking forward to the possible use of undersea fiber optic cables.

III. THE HISTORY OF FISA

If the government overstated telecommunications history in making a case for the PAA, it appears also to have underutilized legislative history.[78] Essentially, the legislative history of FISA shows that the statute was not intended to prevent warrantless surveillance of international communications, except when they were acquired by targeting a particular, known U.S. person in the United States, or when they were acquired from a wire in this country. Surveillance of international communications targeting foreign visitors in the U.S., and non-targeted "vacuum cleaner" surveillance of all international calls (including those made by Americans in the U.S.), was understood to remain firmly outside FISA's regulatory ambit if conducted on radio waves or on wires outside the United States. Congress intended to fill these gaps with subsequent legislation, but never did so.

A. The First Version of FISA.

Over the years leading to FISA's enactment in 1978, three basic versions of the statute emerged.[79] The first would have expanded the criminal wiretapping law, known as Title III, to national security surveillance.[80] Under this approach, FISA essentially would have regulated the interception of all wire and oral communications (and later, electronic communications) in the United States.[81] This version gained little legislative

---

Policies to be Followed in the Authorization of Common Carrier Facilities to Meet North Atlantic Telecommunications Needs During the 1985-1995 Period, 100 F.C.C.2d 1405 & n.16 (1985).

[75] *In re Policy to be Followed in Future Licensing of Overseas Communications*, 71 F.C.C.2d 1090 (1979). The Defense Department did try to persuade the FCC that transatlantic cables "not land in the crowded Northeastern United States corridor." *In re AT&T*, 73 F.C.C.2d 248 (1979). Perhaps DOD would have preferred these cables to make landfall in Canada.

[76] AT&T 1979 Report at 7-8.

[77] AT&T 1976 Report at 9, 11.

[78] Cf. Wainstein Testimony 9-20-07 at 2-4.

[79] Of course, many variations of the bills were introduced and considered at various times.

[80] 18 U.S.C. § 2510 et seq. For a discussion of the interplay between Title III and FISA, see *NSIP* Chapters 7, 14 and 15.

[81] An example of this first model was S. 2820, the "Surveillance Practices and Procedures Act of 1973," which was sponsored by Senator Gaylord Nelson as "a direct response to abuses." *Warrantless Wiretapping and Electronic Surveillance – 1974*, Joint

traction, however, apparently because the government could not tolerate it. As one Member of Congress explained, "in April 1974, when we held hearings on several bills, including a proposal to require a court order prior to any interception of oral or wire communications in foreign intelligence cases … Assistant Attorney General Henry Petersen, speaking for the administration, stated to the subcommittee, 'Let me be very brief. We oppose these bills. That is it.' During the subsequent 2-year period, Mr. Petersen and his successors, as well as intervening Attorneys General, consistently opposed the concept of legislation imposing judicial restraints on foreign intelligence wiretapping."[82]

B. The Second Version of FISA.

The second basic version of the bill, which was supported by the executive branch, would have confined FISA essentially to what are now the last three subsections of 50 U.S.C. § 1801(f), concerning domestic and international (one-end-U.S.) wire communications if acquired inside the United States; domestic radio communications; and techniques such as microphone bugging conducted in the United States.[83] Attorney General Edward Levi testified in favor of a bill of this type in March 1976.[84] He explained that "the definition of electronic surveillance … restricts the scope of the bill to interceptions within the United States," and that it would cover "the use of electronic surveillance to intercept any communication between persons in the United States," but that "government operations to collect foreign intelligence by intercepting international communications … [are] not addressed in this bill."[85] In response to questions, Levi observed that the bill would not apply to "a radio communication of an international kind which is picked up in some kind of a sweeping operation or some other kind of operation,"[86] or to "the transatlantic kinds of sweeping overhearing."[87] In

---

Hearings before the Subcommittee on Administrative Practice and Procedure and the Subcommittee on Constitutional Rights of the Committee on the Judiciary and the Subcommittee on Surveillance of the Committee on Foreign Relations, United States Senate, 93d Cong., 2d Sess. at 256 (Apr. 3 1974, et seq.) [hereinafter FISA Hearings 4-3-74]. In scope, under this bill, FISA would have mirrored Title III. See FISA Hearings 4-3-74 at 274 ("Essentially, the procedures parallel those contained in existing law for wiretaps for domestic crimes").

[82] *Foreign Intelligence Surveillance Act*, Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, 95th Cong., 2d Sess. at 1 (June 22, 1978 et seq.) (statement of Rep. Kastenmeier [hereinafter FISA Hearings 6-22-78]; see *Foreign Intelligence Surveillance Act of 1976*, Hearing before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, United States Senate, 94th Cong. 2d Sess. at 233-265 (Mar. 29, 1976 et seq.) [hereinafter FISA Hearings 3-29-76].

[83] See FISA Hearings 3-29-76 at 1. For a detailed discussion of current 50 U.S.C. § 1801(f), see *NSIP* Chapter 7.

[84] For the language of the bill supported by the Ford administration, see FISA Hearings 3-29-76 at 122-123; *Electronic Surveillance Within the United States for Foreign Intelligence Purposes*, Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Select Committee on Intelligence of the United States Senate, 94th Cong., 2d Sess. at 180-181 (June 29, 1976 et seq.) [hereinafter FISA Hearings 6-29-76].

[85] FISA Hearings 3-29-76 at 11, 20.

[86] FISA Hearings 3-29-76 at 15.

[87] FISA Hearings 3-29-76 at 17.

short, as he made clear,[88] "Congress knows that there is an important area here which is not covered by this legislation."[89]

In subsequent appearances before Congress, Levi repeated these points about the limits of FISA, and referred explicitly to NSA surveillance. For example, he explained that while "one doesn't generally discuss them in public … we do know that there is a kind of sweeping operation by the NSA which is dealing with international communications not covered here. And that is uncovered in this bill."[90] Indeed, Levi summarized testimony given in a closed hearing by the Director of the NSA, General Lew Allen, about "an awesome technology – a huge vacuum cleaner of communications – that had the potential for abuses."[91]

Levi often was quite specific in his testimony, explaining that the bill would not cover surveillance of international communications from radio waves in any location, or from wires located outside the United States, and highlighting the significance of these exemptions for NSA:

> The bill does not purport to cover interceptions of all international communications where, for example, the interception would be accomplished outside of the United States, or, to take another example, a radio transmission

[88] There was some initial ambiguity about whether the bill would apply to international calls "from a citizen in this country, to an agent in a foreign country, a long distance call of that type," because Levi initially affirmed unequivocally that such a call would be within the scope of the statute. FISA Hearings 3-29-76 at 15. In response to later questions, however, he indicated (accurately) that the statute would apply to such communications only when they "involve[] a wire," as opposed to a radio wave, FISA Hearings 3-29-76 at 15, and only when "the tap is placed within the United States," FISA Hearings 3-29-76 at 20.

[89] FISA Hearings 3-29-76 at 25.

[90] *Foreign Intelligence Surveillance Act*, Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary, House of Representatives, 94th Cong. 2d Sess. at 98-99 (Apr. 12, 1976 et seq.) [hereinafter FISA Hearings 4-12-76].

[91] Levi's full summary of Allen's testimony was as follows:

> He described as the responsibility of the NSA the interception of international communication signals sent through the air. He said there had been a watch list [used to select signals for review], which among many other names, contained the names of U.S. citizens. Senator Tower spoke of an awesome technology – a huge vacuum cleaner of communications – that had the potential for abuses. General Allen … said the mission of NSA is directed to foreign intelligence obtained from foreign electrical communications and also from other foreign signals such as radar. Signals are intercepted by many techniques and processed, sorted, and analyzed by procedures which reject inappropriate or unnecessary signals. He mentioned that the interception of communications, however it may occur, is conducted in such a manner as to minimize the unwanted messages. Nevertheless, according to his statement, many unwanted communications are potentially selected for further processing. He testified that subsequent processing, sorting and selection for analysis are conducted in accordance with strict procedures to insure immediate and, wherever possible, automatic rejection of inappropriate messages. The analysis and reporting is accomplished only for those messages which meet specific conditions and requirements for foreign intelligence. The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest.

FISA Hearings 6-29-76 at 28; see FISA Hearings 6-29-76 at 39-40. For public testimony by General Allen concerning NSA's surveillance activities, see *Intelligence Activities, Senate Resolution 21*, Hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, 94th Cong., 1st Sess., Volume 5 at 1-55 (Oct. 29, 1975 et seq.) [hereinafter Church Hearings, Volume 5].

> that does not have both the sender and all intended recipients within the United States.
>
> Interception of international communications, beyond those covered in the bill, involves special problems and special circumstances that do not fit the analysis and system this bill would impose. This is not to say that the development of legislative safeguards in the international communications area is impossible. But I know it will be extremely difficult and will involve different considerations.[92]

In response to a Senator's question about "what is covered by this legislation," Levi replied, "it has to come under the definition of electronic surveillance. If it doesn't come under that, it goes beyond that, then we say, well, it is outside the scope."[93] Asked whether "we really [are] talking about the thrust of the whole NSA program," Levi replied, "We are talking about that portion of the NSA program which is not covered here, and which as I say, I really don't want to discuss in any detail," but which Senators had discussed with the NSA the previous day in executive session.[94] He went on to say that "I know you had an executive session. A great deal of that is not covered by the definition."[95]

---

[92] FISA Hearings 6-29-76 at 80.

[93] FISA Hearings 6-29-76 at 111.

[94] FISA Hearings 6-29-76 at 111.

[95] FISA Hearings 6-29-76 at 111. Although classified testimony about the NSA's surveillance capabilities is unavailable, there was open testimony in the Senate that is relevant. David Watters, a telecommunications engineer and former employee of the CIA and Western Electric (the engineering division of AT&T), described in great detail the surveillance methods used by the government for "broadband interception."

> By broadband interception we mean that kind of wiretapping wherein the government places electronic surveillance on a large number of parallel communications circuits simultaneously. This practice may be done by interception of major trunk lines within or between cities. … It is being done by interception of major cross-country microwave link pinch points each containing tens of thousands of message circuits. This is in addition to similar surveillance on the primary U.S. electronic portals for foreign telecommunications traffic.…
>
> Today the federal government is stalking at random throughout our telecommunications common carrier circuits. In most cases, this is being done without a court order. In the greater majority of these intercepts, there is no specific order from the Attorney General. Rather, this activity is being done on a blanket order….
>
> [O]ne must observe that a broadband intercept surveillance operation injected into a single microwave link, for instance, permits the scanning of hundreds of thousands of messages in a single day with sophisticated computer-like equipment operated unattended, or by one or two persons.…
>
> It must be understood that when a warrant would be issued for a certain targeted objective to be sought through the broadband system, this does not ordinarily mean that special equipment is installed for that objective alone. The equipment is already in place in our microwave long lines network. What it really means is that a new set of punched cards are inserted into the system to operate as a new addition to the watch list of called telephone and telegraph numbers or to the trigger word lexicon.

Foreign Intelligence Surveillance Act of 1977, Hearings before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, United States Senate, 95th Cong. 1st Sess. at 118-119 (June 13, 1977 et seq.) [hereinafter FISA Hearings 6-13-77]. Similar testimony from Mr. Watters appears in *Foreign Intelligence Surveillance Act*, Hearings before the

Similar points were made by other witnesses,[96] perhaps most powerfully by Morton Halperin, who himself had famously been the target of an extensive national security wiretap. As Halperin explained to the Senate Judiciary Committee, "[w]hat seems to be at stake here in these very artfully drawn words," defining the term "electronic surveillance," is "the activities of the National Security Agency."[97] Halperin testified that the NSA was then monitoring international communications, and that the bill would allow such monitoring to continue:

> this bill, as I read it, would not cover phone conversations from an American citizen in the United States to a foreign country, if it goes by microwave, or if it passes through Canada, even if it does not go by microwave, because the definition in the bill of electronic surveillance says that it covers wire communication[s] only where the acquisition occurs within the United States while the communication is being transmitted by a wire; so that if the acquisition was from a cable underneath the ocean, it would not be covered. If the acquisition occurred while the material passed through Canada, it would not be covered and if the acquisition occurred under microwave, it would not be covered. It is explicitly stated when you deal with a radio transmission that it is only included if the point of origin and all attendant [sic] recipients are within the United States. So that a phone conversation abroad would not be covered by this bill.[98]

In response to questions, Halperin reiterated that "if I am an American citizen [in the United States] and I make a phone call to London, and the Government picks it up on a transatlantic cable under the ocean, it is not covered."[99] Thus, he testified, "it seems to me clear that the intent is to exclude the acquisition of messages from the United States [to] abroad which are picked up either in the air or picked up overseas, or on their cables that go under the ocean."[100]

One of the most explicit (and astute) analyses of the limits in the bill came from Philip Lacovara, a former Justice Department official. He explained:

Subcommittee on Intelligence an the Rights of Americans of the Select Committee on Intelligence of the United States Senate, 95th Cong., 2d Sess. at 148-178 (July 19, 1977 et seq.) [hereinafter FISA Hearings 7-19-77].

[96] Philip Heymann, a professor at Harvard Law School, testified that "[t]he statutory definitions are highly specific and are plainly limited to domestic taps. There is no question about that." FISA Hearings 3-29-76 at 57; see FISA Hearings 6-29-76 at 175-176. See also FISA Hearings 6-29-76 at 201 (statement of Senator Mondale); FISA Hearings 6-13-77 at 50 ("This bill [S. 1566] that you are considering today does not apply to surveillance activities conducted outside the United States" (statement of Secretary of Defense Harold Brown)).

[97] FISA Hearings 3-29-76 at 31.

[98] FISA Hearings 3-29-76 at 31.

[99] FISA Hearings 3-29-76 at 32.

[100] FISA Hearings 3-29-76 at 32.

> the tapping of any wire communication (telephone, telegraph, telex, etc.) is covered if either the sender or receiver is in the United States [and the wiretap occurs in the United States]. I leave to the experts whether present or foreseeable technology will allow the interception of wire communications wholly within the United States from a point outside the United States; if so, they would not be covered. Since the bill deals only with interceptions taking place in the United States. More clearly not covered are international wire communications since it is relatively simple, I understand, to intercept these communications at a point outside the United States.
>
> Similarly, radio communications are covered only if both the point of origin and of intended receipt are within the United States and only if made "with a reasonable expectation of privacy." Quite obviously, therefore, the bill would have no application whatsoever to international radio traffic, even of a private or commercial nature.[101]

In sum, Congress was told, repeatedly and explicitly, by the Attorney General and other current and former government officials, that the second version of FISA contained large loopholes designed primarily to accommodate NSA's signals intelligence activities. Foreign intelligence wire surveillance of international communications conducted outside the United States, and radio surveillance of international communications conducted inside or outside the United States, would remain unregulated by statute, even if the communications were to, from, or about U.S. persons in the United States, and even if a U.S person in the United States was the target of the surveillance.

C. The Third Version of FISA.

In an apparent effort to assuage concerns arising from these limits, the third and final basic version of FISA was introduced in 1977. It retained the three-part definition of "electronic surveillance" from the prior version, but added a fourth part similar to what is now 50 U.S.C. § 1801(f)(1).[102] This new language extended FISA to surveillance targeting any "particular, known, United States person who is in the United States," regardless of whether the surveillance involved domestic or international communications, whether those communications were acquired from a wire or radio wave, and whether the surveillance occurred inside or outside the U.S.[103]

Attorney General Griffin Bell, who had succeeded Levi, explained that the new language "closes a gap that was present in last year's bill by which Americans in the

---

[101] FISA Hearings 4-12-76 at 8; see also FISA Hearings 4-12-76 at 16; FISA Hearings 6-29-76 at 134; *Foreign Intelligence Electronic Surveillance*, Hearings before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence, House of Representatives, 95th Cong., 2d Sess. at 206-207 (Jan. 10, 1978 et seq.) [hereinafter FISA Hearings 1-10-78].

[102] See 50 U.S.C. § 1801(f)(1).

[103] FISA Hearings 6-13-77 at 136-137.

United States could be targeted for electronic surveillance of their international communications. In this bill, such targeting will require a prior judicial warrant."[104] This alone is powerful evidence that some of the limits of FISA were then understood.

Although he characterized the new language as a gap-filler, Bell made clear that it applied only to surveillance "intentionally" targeting particular, "known" U.S. persons in the United States, giving examples of cases that would remain outside the scope of the bill.[105] Defense Secretary Harold Brown elaborated on Bell's testimony as it applied to the NSA. With respect to the "known" person standard, Brown explained that "many of these channels of communication [that the government monitors] are used by a great many people," and so "it cannot be said in advance who the individuals are."[106] In other words, as the Defense Department's general counsel put it, "[t]his is intended to get at a problem that we have with bulk communications.… Those are communications which are not simply from one person to another person or one entity to another entity, but they include large numbers of communications and large numbers of subjects."[107]

Again, Mort Halperin clearly identified the limits in the new proposal. He explained that NSA "could put the word 'terrorism' into its computer and then read every cable that mentions the word 'terrorism,' whether it is addressed to an American citizen or from an American citizen [or] even if it is from one American citizen to another American citizen, provided one of them is outside the United States."[108] In other words, the NSA could not target particular Americans in the United States – *e.g.*, by using identifying selectors, such as names or social security numbers, in its watchlists. But it could use subject-matter selectors, such as "terrorism," even though they inevitably would acquire many Americans' communications. And if those communications contained foreign intelligence, NSA could retain and disseminate them in the usual

[104] FISA Hearings 6-13-77 at15; see also FISA Hearings 1-10-78 at 9 (statement of Attorney General Bell). As Bell later put it in testimony before the House Intelligence Committee, "a prior judicial warrant is now required for all targeting of Americans in the United States for electronic surveillance of their international communications" as well as their domestic communications. FISA Hearings 1-10-78 at 15.

[105] Bell justified this limitation with three examples. First, he explained, when the government monitors radio communications, "the identity of the person involved [may be] totally unknown and largely undiscoverable," and indeed a "high priority of this [surveillance] activity is in fact to discover the identity of the communicator." FISA Hearings 6-13-77 at 6. Bell assured Congress, however, that if an intelligence agency found "that the person was a United States person, [and] … failed immediately to obtain a warrant – if a warrant were required for law enforcement purposes – officials of the agency would be criminally liable…." FISA Hearings 6-13-77 at 6. Second, in some cases, unbeknownst to the Intelligence Community, a foreign government official may be a U.S. person, and "the qualifier 'known' is required to keep such a mistake from becoming a criminal offense." FISA Hearings 6-13-77 at 6. Third and finally, Bell explained that "agencies operating totally overseas and targeted solely against foreign communications can, through the quirks of radio communications, accidentally intercept radio communications which are intended to be wholly domestic within the United States. Over time there is a statistical certainty of this occurring at uncertain and generally infrequent intervals." FISA Hearings 6-13-77 at 6.

[106] FISA Hearings 6-13-77 at 68.

[107] FISA Hearing 6-13-77 at 68.

[108] FISA Hearings 6-13-77 at 98.

ways.[109] As the Senate Intelligence Committee later explained in a report on the first five years of FISA's use:

> The greatest challenge to those responsible for oversight of intelligence surveillance operations has been to devise means to accommodate the privacy interests of U.S. persons given the technical capabilities of the SIGINT system to provide information based on topical interests. Without targeting any particular U.S. persons [*e.g.*, without using identifying selectors, such as names], SIGINT collection operations inevitably give NSA direct access to international and foreign communications of and about U.S. persons [because those communications are retrieved by subject-matter selectors, such as "terrorism"].[110]

---

[109] As one witness explained, "[t]he clever usage of the phrase 'acquired by intentionally targeting that United States person' is perpetuated in S. 1566 …. The key word is 'targeted,' not 'intercepted.' …. In actuality, the technology being employed identifies targeted trigger words in thousands of telegraphic or data messages, or identifies peculiar signals associated with telephone calls as they pass through the dragnet. An automatic recorder then snatches out the while message for later examination by agents. Thus, it is not 'persons' who are the primary targets of these insidious kinds of surveillance, rather it is 'information' which is targeted. Small consolation that the private communications of innocent citizens are sucked up into the NSA vacuum cleaner!" FISA Hearings 7-19-77 at 154 (statement of David Watters).

More recently, a company known as Pudding Media, founded by two former members of "an elite R&D unit of the IDF [Israeli Defense Force]," Pudding Media, About Us (available at http://puddingmedia.com/about_us.html), claims to be able to scan VOIP calls for keywords, and direct targeted advertising to callers:

> When certain keywords are spoken, interesting and timely news, entertainment, and offers are displayed on the [computer] screen [of the computer being used in the VOIP call]. For example, a consumer talking about movies may see links to trailers, reviews and show times for nearby theaters. A sports fan talking about a favorite team may see commentary and game statistics on a computer or handset screen.

Pudding Media, Press Release (9-24-07) (available at http://puddingmedia.com/news/press/pr20070924.html). For a discussion of Pudding Media and its technology, see Louise Story, Company Will Monitor Phone Calls to Tailor Ads, *New York Times* (9-24-07).

[110] *The Foreign Intelligence Surveillance Act of 1978: The First Five Years*, S. Rep. No. 98-660, 98th Cong., 2d Sess. at 21 (1984) [hereinafter FISA Senate Five Year Report]. The Senate Intelligence Committee announced its intent to deal with this issue by requesting periodic reports on "non-FISA search and surveillance techniques against persons in the United States or U.S. persons abroad that would require a warrant if used for law enforcement purposes." FISA Senate Five Year Report at 22-23.

Congress understood that subject-matter selectors could be used on the international communications of Americans located in the United States, as illustrated by the following exchange between Halperin and Senator Kennedy:

> SENATOR KENNEDY: That is the overseas problem.
>
> MR. HALPERIN. No; it is not. A person can be in the United States. If you are in the United States and you send a cable, the only part of that that is covered is the business that we talked about this morning of known U.S. persons.
>
> The definition of electronic surveillance on page 6 [of the bill], beginning on line 15(a)[110] is acquisition of radio [or] wire communications that go overseas only if sent or received by a particular known U.S. person.
>
> If they are intercepting every cable that moves over a wire, say, between New York and London –
>
> SENATOR KENNEDY. We are concerned about that. I am hopeful we can get together with Senator Bayh and others. You are pointing out an area that is a matter of concern for us.
>
> MR. HALPERIN. This is not overseas. This is somebody in the United States [sending a message abroad].

In his testimony on the third version of FISA, Philip Lacovara also emphasized the narrow reach of the bill, and the possible reasons why it was so narrow:

> The types of "electronic surveillance" that would be regulated under H.R. 7308[111] are rather cleverly defined … to focus on *certain* purely internal United States communications or on interceptions taking place within the United States. Some types of electronic intelligence gathering would not be covered at all, however, and the Subcommittee should understand that the bill is *not* all encompassing. For example, if the interception is not physically made in the United States, broad scale monitoring of international radio and cable traffic would be unregulated so long as no particular citizen or resident alien is being targeted. This allows "vacuum cleaner" methods of intelligence collection to take place without control. In addition, the interception of purely domestic wire transmissions would not be covered if technology permits the interception to be done outside United States territory – *e.g.*, by surveillance ship off shore or by satellite.…
>
> These definitions have clearly been crafted to leave many types of intelligence collection activities completely *outside* the coverage of the bill. I confess to continuing skepticism about the justification for complete exemption of these activities. If these omissions are to be preserved, the Subcommittee should insist on some convincing explanation from the intelligence agencies for adopting a selective approach to the regulation of ELINT (electronic intelligence) collection.[112]

In sum, even the third and final basic version of FISA contained loopholes designed to accommodate the NSA. The statute would not regulate wire surveillance of international communications conducted outside the United States, or radio surveillance of international communications in any location, even if the communications in question were to, from, or about U.S. persons in the United States – as long as the surveillance did not target any particular, known U.S person in the U.S. And Congress was told expressly that watchlist surveillance using subject-matter selectors, such as "terrorism," would not be deemed to target any particular, known U.S. person, even if it inevitably acquired vast numbers of communications made by U.S. persons.

FISA Hearings 6-13-77 at 98. See also FISA Hearings 1-10-78 at 146, 163-164. Senator Kennedy evidently absorbed this, because when he later testified before the House Intelligence Committee, he explained: "What is not covered by this bill are U.S. citizens abroad … and nontargeted sweeps by the NSA. But targeted sweeps [involving U.S. persons in the U.S.] would be covered by this bill." FISA Hearings 1-10-78 at 172.

[111] For the text of H.R. 7308, see FISA Hearings 1-10-78 at 240-241.

[112] FISA Hearings 1-10-78 at 206-207 (italics in original).

D. The Committee Reports on FISA.

The final committee reports on FISA are not as explicit or detailed, but nonetheless confirm the account set forth above. For example, discussing the first part of the definition of "electronic surveillance,"[113] the Senate Intelligence Committee's report announced that FISA would "protect[] 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."[114] This included NSA "watchlisting" activities directed at U.S. persons located in the United States.[115] But the report explained that Subsection (1) "does not apply to the acquisition of the contents of international or foreign communications, where the contents are not acquired by intentionally targeting a particular known U.S. person who is in the United States."[116] And it went on to explain that the remaining provisions of the definition would apply to surveillance of a wire inside the United States, even if one party to the communication was abroad, but that surveillance of a "microwave radio transmission is meant to be covered … [only] if the sender and all intended recipients are located within the United States, or … if it is done through the targeting of a U.S. person who is in the United States."[117] Both Senate reports on FISA also observed that "most telephonic and telegraphic communications are transmitted at least in part by microwave radio transmissions."[118]

The reports also made clear Congress' intent to fill the gaps left by FISA. The Congressional committees were "concerned" about the limits of FISA,[119] found it "desirable to develop legislative controls" over the NSA's signals intelligence activities,[120] and had at least one bill to do so under consideration.[121] But they did not want that broader project to derail the incremental progress represented by FISA.[122]

---

[113] 50 U.S.C. § 1801(f)(1).

[114] S. Rep. No. 95-701 at 33-34 (1978) (italics in original).

[115] S. Rep. No. 95-701 at 34 (1978).

[116] S. Rep. No. 95-701 at 34 (1978).

[117] S. Rep. No. 95-701 at 35 (1978). Similar language appears on pages 32-34 of the Senate Judiciary Committee's report, S. Rep. No. 95-604 (1978).

[118] S. Rep. No. 95-604 at 33; S. Rep. No. 95-701 at 35.

[119] S. Rep. No. 95-701 at 34.

[120] S. Rep. No. 95-604 at 34.

[121] S. Rep. No. 95-701 at 35 (citing S. 2525).

[122] The reason civil libertarians supported FISA was summarized by Halperin:

> Well, I have mixed feelings about that. I think it's important for Congress to legislate about the National Security Agency and it may be that this is the appropriate occasion, and it should be taken. On the other hand, if one had a bill which really brought wiretapping within the United States under effective safeguards and eliminated the existent situation in which it is done without any controls at all and the only problem with the bill was the NSA issue, I

And they made clear that the gaps in FISA eschewing regulation of NSA SIGINT collection "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans."[123] In the end, of course, the gaps were not filled. One reason appears to be that the subsequent surveillance legislation became entangled in the doomed effort to establish legislative charters for the Intelligence Community.[124] Another reason, of course, may be that some of the gaps were closed by the very technological and other operational developments that the government now cites in support of the PAA and the FAA.[125]

In 1978, however, FISA clearly left the government free to monitor international communications, including communications to or from Americans, using radio surveillance of microwave satellite signals, or wire surveillance of transoceanic cables on foreign soil or offshore, as long as it did not target any particular, known American who was located in the United States. As far as the statute was concerned, vacuum-cleaner watchlisting by subject-matter, rather than by name or other identifier, remained available on radio waves and on wires outside the United States, even with respect to the international communications of Americans located in the United States.

E. The Anomaly of FISA's Second Subdefinition of "Electronic Surveillance".

The account set forth above is hard to dispute, because the legislative history is so explicit. But it is also difficult to square with what is now the second part of the definition of "electronic surveillance,"[126] a provision that, beginning with the second version of the bill, applied to wire surveillance in the United States of a communication "to or from" a person located in the United States. The legislative history of this provision "makes clear [that] one party to the wire communication may be outside the United States if the acquisition occurs within the United States. Thus, either a wholly domestic telephone call or an international telephone call can be the subject of electronic surveillance under this subdefinition if the acquisition of the content of the call takes place in this country."[127]

> guess I would come down saying, "Let's move on the surveillances within the United States and move NSA in a separate bill."

FISA Hearings 4-12-76 at 50. Attorney General Griffin Bell also stated the Justice Department's commitment to drafting such additional legislation, FISA Hearings 7-19-77 at 16; see also FISA Hearings 1-10-78 at 11-12.

[123] S. Rep. No. 95-701 at 35.

[124] For a discussion of this effort, see *NSIP* Chapters 1 and 2.

[125] See discussion in Part III.f, *infra*.

[126] 50 U.S.C. § 1801(f)(2) provides that "electronic surveillance" includes "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" (emphasis added).

[127] H.R. Rep. No. 95-1283, Part I at 51.

If Congress genuinely intended to permit warrantless surveillance of international calls as described above, why did it not confine this second part of the definition to communications "to and from" persons in the United States, instead of "to or from" such persons? It easily could have written the second part of the definition to match the third, which explicitly applies only to domestic radio communications – radio communications where "both the sender and all intended recipients are located within the United States."[128] Put another way, why would Congress want to require a warrant for wire surveillance of international communications conducted inside the U.S., when no warrant was required for wire surveillance of international communications conducted outside the U.S. (except when it targeted a particular, known U.S. person in the United States)?

The record I have reviewed does not answer the question authoritatively; the language that became the second part of the definition of "electronic surveillance" was included in the first bill supported by (and apparently drafted by) the Ford administration,[129] and its application to wire surveillance in the United States was never seriously challenged. But there is one possible explanation. Congress was focused on protecting domestic communications, and perhaps it thought that wire surveillance inside the United States, even if nominally directed at international traffic, carried with it an inherently greater risk of acquiring domestic communications. By pushing warrantless wire surveillance offshore, Congress could be more certain it would not include domestic communications, either by accident or otherwise, because (as I understand it) domestic communications generally did not transit on cables located outside the United States.

For its part, the government may not have objected to a warrant requirement for international wire communications acquired in this country. This might have been true for any of three reasons: first, because surveillance of a target in this country would likely seek domestic as well as international communications, requiring a visit to the FISA Court in any event; second, because surveillance of a target located abroad would probably occur abroad, thus not implicating the limits on surveillance of domestic wires; and third, perhaps because surveillance of a cable outside the United States was then thought to be the best way to target international wire communications – i.e., more efficient, or at least more possible, than conducting wiretaps inside the U.S. offices of the telephone company.[130]

---

[128] 50 U.S.C. § 1801(f)(3) provides that "electronic surveillance" includes "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" (emphasis added). As noted above, by contrast, 50 U.S.C. § 1801(f)(2) applies to communications "to or from a person in the United States."

[129] FISA Hearings 3-29-76 at 1 ("S. 3197 is identical to a measure transmitted to the Senate by the President on March 23, 1976, with a message urging its enactment"), 122-123 (operative language of S. 3197).

[130] In the 1970s, NSA appears to have used self-help surveillance, without substantial aid from the telephone companies, for its main surveillance operations. Cf. 18 U.S.C. § 2518(4) (enacted in 1968). Indeed, one of the reasons the executive branch supported FISA was the fact that the telephone companies were balking at cooperating with the government. See Memorandum re. Possible Amendments to FISA, to Dan Levin, Office of the Deputy Attorney General, from Mary Lawton, Counsel for Intelligence Policy at 4 (Nov. 1, 1990) (released in redacted form by the Department of Justice under the Freedom of Information

Alternatively, it may be the case that NSA simply miscalculated, believing that another provision,[131] added to FISA at the last minute and supported by closed testimony,[132] would give it sufficient authority. As first proposed, near the end of the legislative debates on FISA, this provision would have permitted warrantless wire surveillance in the U.S. if the surveillance was "solely directed at … communications exclusively between or among foreign powers."[133] NSA may have believed it could use this authority aggressively, perhaps even adopting some kind of modified "vacuum cleaner" approach, as long as it could credibly claim that the targets of the surveillance were foreign powers. A mere twenty days before the bill became law, however, the House-Senate Conference Committee imposed two additional requirements that foreclosed any broad reading of the provision. These were, first, a requirement that the surveillance be directed solely at "means of communications" – rather than merely "communications" – used exclusively between or among foreign powers; and second, a requirement that the Attorney General certify that the surveillance created "no substantial likelihood" of acquiring a U.S. person's communications.[134] These two requirements essentially limited the provision to foreign government hotlines and other dedicated channels.[135]

F. NSA's Technical Problems and Legislative Solutions.

Act in October 2007, and on file with the author) [hereinafter Possible FISA Amendments Memo 11-1-90]. In the hearings on FISA, a representative of AT&T testified as follows:

> In cooperating with court-ordered and national security cases we believe that our proper role, as a communication common carrier, is to provide the minimum assistance necessary to effectuate the particular wiretap, whether of voice or non-voice communications. Under no circumstances do we do any of the ensuing monitoring or recording; that, in our opinion, is the exclusive province of the appropriate law enforcement officers.
>
> Nor do we furnish them with any terminal equipment to be used in connection with their wiretap.…
>
> Nor do we design or build wiretap or eavesdrop devices for law enforcement authorities.
>
> Nor do we allow them to enter our central offices.
>
> Nor do we train law enforcement personnel in the general methods of wiretapping and eavesdropping.
>
> Nor do we provide telephone company employee identification cards, uniforms or tools, or telephone company trucks.

FISA Hearings 6-22-78 at 103 (statement of H.W. William Caming, Attorney, AT&T). Surveillance of an undersea cable, rather than in AT&T's offices, accords with this account. Since then, of course, times have changed, and the PAA's main provision applies only when the government is proceeding with the aid of a communications provider or other third party. See 50 U.S.C. § 1805B.

[131] 50 U.S.C. § 1802.

[132] See H.R. Rep. No. 95-1283, Part I at 68 (1978).

[133] H.R. Rep. No. 95-1283, Part I at 4 (text of bill), 68 (discussion of bill) (1978).

[134] See H.R. Rep. No. 95-1720 at 24 (1978).

[135] For a discussion of Section 1802, see *NSIP* Chapter 12.

As far as I can tell, NSA's technological problems in this area were recognized at least as early as 1987, a year before the first transatlantic fiber optic cable went into service.[136] In 1990, DOJ's Office of Intelligence Policy and Review (OIPR) wrote a memo to the Office of the Deputy Attorney General explaining that it had been "working with the National Security Agency for the past three years to develop possible amendments to the Foreign Intelligence Surveillance Act to meet a need created by technological advances."[137] In particular, these technological advances appear to have affected "NSA's collection of international and foreign communications,"[138] creating a "practical imperative" for legislation.[139] The 1990 memo cited draft legislation on which DOJ and the NSA were "close to agreement," and which would have "provide[d] for Attorney General certification, rather than court order" for the surveillance.[140]

However, the 1990 memo also identified several "policy and tactical issues" counseling against seeking new legislation. Among those issues were the following:

- the fact that "committee jurisdiction in both the House and Senate is concurrent between the Intelligence and Judiciary Committees," and while the "problems giving rise to the possible amendments have all been discussed with the Intelligence Committees," they had not been discussed "with the Judiciary Committees";

- concerns about separation of powers, and the question whether "putting the proposed new collection under the statute, albeit on the basis of Attorney General certification, pose[s] greater separation of powers problems than attempting to exclude the collection from the statute?"

- "the risk of added congressional restrictions if the statute is opened up to amendment"; and

- the fact that "the proposed amendment to FISA to resolve the NSA problem … is certain to be written in such enigmatic terms that only those who have been

[136] See FCC Trends Report 1997 at 25 (table 11). See *In re. AT&T et al.*, 98 F.C.C.2d 440 (1984) (order authorizing TAT-8).

[137] Possible FISA Amendments Memo 11-1-90 at 1. Redactions in the memorandum make it difficult to identify the precise nature of NSA's technological problem, but it clearly had to do with FISA's definition of "electronic surveillance." Possible FISA Amendments Memo 11-1-90 at 1-2. I should note that the Freedom of Information Act request that produced this memorandum was not filed in connection with this paper (it was sent to DOJ in May 2005 in connection with *NSIP*).

[138] Possible FISA Amendments Memo 11-1-90 at 1.

[139] Possible FISA Amendments Memo 11-1-90 at 4. The memo explained that concerns about the 1978 version of FISA were overcome by the "practical imperative of continuing to collect foreign intelligence in the face of growing resistance from the communications common carriers whose cooperation was essential." Possible FISA Amendments Memo 11-1-90 at 4. The memo reported that "NSA views the changing technology as creating a similar practical imperative," and that "it could also be considered a legal imperative since the existing statute prohibits … the collection NSA is seeking." Possible FISA Amendments Memo 11-1-90 at 4.

[140] Possible FISA Amendments Memo 11-1-90 at 1, 3.

> briefed in executive session will understand them," thus risking "speculation in the media about what is really intended and probably deep suspicion that something sinister is going on."[141]

These policy and tactical issues appear to have overcome the practical imperative in 1990, resulting in no amendments to FISA. By 2007, however, the policy and tactical issues had receded – or the practical imperative had increased – and the government sought an expansion of its authority in the FISA Modernization Act,[142] a limited version of which later became the PAA.

IV. CURRENT ISSUES

The telecommunications and legislative history described above is (I hope) relevant to current debates. But of course it is not determinative. Each generation of Americans is responsible for making its own judgments, as Judge Royce Lamberth, the former Presiding Judge of the FISA Court, has explained:

> Like many competing American values, liberty and security converge in law. We strike the balance between them not only in the many particular statutes, orders, and policies of the government, but also in the ongoing process of Legislative, Executive, and Judicial action – and reaction – within the framework prescribed by the Constitution. Our national security is therefore cast, and continually recast, in the crucible of our legal system.[143]

FISA was one recasting of the balance between liberty and security, the PAA was another, and any successor legislation will be a third.

Today, I think the central operational problem in foreign intelligence surveillance is the difficulty of determining, at least in real time, the location of communicating parties who do not wish to be found. This problem stems in large part from changes in telecommunications technology and globalization, including the advent of web-based and other Internet-based communications, mobile communications devices, packet-switched networks, and increased international travel.[144] In 1976, for example, only

---

[141] Possible FISA Amendments Memo 11-1-90 at 4-5.

[142] See, *e.g.*, Proposed FISA Modernization Act Section 402 (available at http://intelligence.senate.gov/070501/bill.pdf); Letter from David S. Kris to the Senate Select Committee on Intelligence at 35-39 (May 1, 2007) (available at http://intelligence.senate.gov/070501/kris.pdf).

[143] *NSIP* Preface.

[144] See Statement of James Baker before the Senate Judiciary Committee (Sept. 25, 2007) (describing the situation in which "you cannot tell in advance (if ever) where one or both of the parties to a communication are located. This is a particular issue with Internet communications, including web-based email, as well as mobile telephone technology.") (available at http://judiciary.senate.gov/testimony.cfm?id=2942&wit_id=6669). For a detailed account of this problem from technical experts, including Susan Landau of Sun Microsystems, see Steven M. Bellovin et al., *Risking Communications Security: Potential Hazards of the 'Protect America Act'* (Oct. 24, 2007) (draft paper available at http://research.sun.com/people/slandau/PAA.pdf) [hereinafter Hazards Draft Paper]. This paper explains in some detail the "surprisingly difficult problem" of identifying in real time "whether [a] communication starts or ends outside the United States," both on the Internet and on the telephone network,

"about 25 percent" of U.S. telephone subscribers could make international calls without operator assistance.[145] Now, essentially everyone in the United States can dial direct, and many use technologies such as VOIP and instant messaging.[146] Similarly, in 1975, approximately 6 million airline passengers arrived in the United States from foreign countries; in 2005, the number had grown to approximately 29 million.[147]

This operational difficulty gives rise to what I think is the central policy question presented today: when, and under what circumstances and conditions, should the government be allowed to conduct large numbers of national security wiretaps, for long periods of time (more than 72 hours), without individualized findings of probable cause made in advance by judges?[148] Previously, FISA answered that question largely by resort to geographical criteria. As changing technology and globalization nudge those criteria towards obsolescence, we may need to identify a new approach.

The next paragraphs discuss these operational and policy issues, including their resolution in the PAA, as applied to (A) foreign-to-foreign communications; (B) international communications, with one end in the United States; and (C) domestic communications. There appears to be broad consensus that foreign-to-foreign communications should be exempt from FISA, and broad consensus that domestic communications should not be exempt. In theory, therefore, the dispute centers on international communications to or from the United States. In practice, however, it extends further because of the difficulty of determining the location of parties to a communication.

A. Foreign-to-Foreign Communications.

FISA has never regulated surveillance of wire or radio communications transmitted between two parties abroad. For example, if a U.S. citizen travels to Paris and telephones a friend in London, the U.S. government has always been able (as a legal matter) to monitor the call without a warrant under FISA. And that has always been the case regardless of where the government did its monitoring – i.e., even if the call was routed through the United States and wiretapped here.[149]

---

and discusses how "NSA has worked on the problem, and … even has a patent for using time latency to determine a communication's location."

[145] AT&T 1976 Report at 11.

[146] For a more complete discussion of technological changes and other issues in telecommunications, see, *e.g.*, W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press 2007).

[147] U.S. Department of Transportation, Bureau of Transportation Statistics, National Transportation Statistics (2007) (available at http://www.bts.gov/publications/national_transportation_statistics/pdf/entire.pdf).

[148] See David Kris, Slate Discussion, Post # 3. As explained in the Slate Discussion, this policy question has been expressed not only through the PAA, but also through the TSP and the January 2007 FISA Court orders. Some of the language in this paper is drawn from the Slate Discussion.

[149] For a detailed explanation of why this is so, see *NSIP* Chapter 7.

These foreign-to-foreign telephone calls were (and still are) simply outside the reach of FISA, and there is widespread agreement that this is appropriate. As General Hayden testified before Congress in 2006, "we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that get[] routed through US facilities."[150] Similarly, Kate Martin and Lisa Graves have acknowledged that "in crafting FISA Congress did not intend to place rules on the monitoring of what has been called 'foreign-to-foreign' communications."[151]

Over time, however, changing technology has brought at least one form of foreign-to-foreign electronic communication within FISA's scope. Prior to the PAA, the government could not conduct warrantless surveillance in the U.S. of stored e-mail messages exchanged between two parties located abroad.[152] That scenario is possible because many Internet Service Providers – AOL, Microsoft, Google – store e-mail messages on giant computers (known as servers) inside this country. If a person in Paris checks his Hotmail account from a cybercafé, he may be connecting to a server located in Redmond, Washington. Prior to the PAA, if the U.S. government acquired his e-mail from that server, it was subject to FISA. Indeed, FISA applied even if all of the e-mail messages in question had been exchanged between the person in Paris and another person in London, and even if both persons were foreigners.[153]

It appears that nearly everyone who understands this problem agrees that it compels a legislative solution. There is no reason to distinguish between foreign-to-foreign e-mail messages acquired from servers located in the United States, and foreign-to-foreign telephone calls acquired from switches located in the United States. If the latter are exempt from FISA, the former also should be exempt.

As it turns out, however, the difficulty of determining location makes it difficult, if not impossible, to fashion a narrowly tailored solution to the problem of foreign-to-foreign e-mail. The main issue (though not the only one) is that people can read and write e-mail from anywhere – whether it be from their homes in New York City, or from a cybercafé in Paris, France. That makes it very difficult to amend FISA in a way that exempts only foreign-to-foreign e-mail messages, but not e-mail messages to or from persons located in the United States. The same may be true of some mobile

[150] Hayden Testimony 7-26-06.

[151] Martin-Graves Statement 5-1-07 at 13. Martin and Graves appear not to object to Congress's decision, but I do not wish to overstate their views.

[152] For a detailed explanation of why this is so, see *NSIP* Chapter 7 (at Section 7:30); see also David Kris, Slate Discussion, Post # 3.

[153] See 50 U.S.C. § 1801(f)(4); *NSIP* Chapter 7.

telephones, as the NSA has explained,[154] and of certain VOIP services, as the FCC has explained.[155]

To understand this problem in practical terms, consider that when the government copies an e-mail message from a server, it may not know where the recipient of the message is located. Indeed, depending on how frequently the recipient checks his e-mail, the government may read the message before he does. An exemption for foreign-to-foreign communications does not solve the problem in that situation, at least if geographical uncertainty is to be resolved against the government.

A related problem is that many persons abroad may exchange e-mail not only with other foreign locations, but also with the United States. Surveillance of such a person's e-mail account will acquire both types of messages. A FISA exemption limited to foreign-to-foreign communications therefore effectively leaves in place the requirement for a warrant for every (or almost every) overseas target using an ISP in the United States, both because (or at least to the extent that) the government cannot quickly segregate the foreign-to-foreign messages, and because in any event it cannot afford to ignore the messages sent to or from the U.S.

Finally, and stated more generally, the problem is that foreigners abroad can now communicate inside U.S. cyberspace. This presents a strange constitutional combination of seemingly unprotected persons (foreigners with no ties to the U.S. except an e-mail account with an American ISP)[156] using highly protected facilities (the U.S. servers of the American ISP) to correspond with one another. That combination tends to frustrate both the U.S. Intelligence Community, which feels the need to search aggressively within those facilities in an effort to root out the terrorists, and civil libertarians, who fear that such rooting around inevitably compromises the privacy interests of innocent Americans who are by far the majority users of those facilities. It also may help explain the puzzlement that each side of the current policy debate apparently feels about the other's position.

B. International (One-End-U.S.) Communications.

The PAA exempts from FISA not only foreign-to-foreign communications, but also international communications to or from the United States, including telephone calls and e-mail messages. If the surveillance is "directed at" a person (reasonably

[154] As stated by the Director of the National Security Agency, in an era of mobile phones, "telephone area codes are less reliable indicators of the physical location of their users." Alexander QFRs 12-19-06 (answer to Question 20 for Senator Feingold).

[155] In its Consumer Advisory: VoIP and 911 Service (available at www.fcc.gov/cgb/consumerfacts/voip911.pdf), the FCC explains that "Interconnected VoIP service allows you to make and receive calls to and from traditional phone numbers, usually using an Internet connection." While "[t]raditional phone services have generally associated a particular phone number with a fixed address," some "interconnected VoIP services enable customers to take their home or business phone almost anywhere" that they can get a connection to the Internet. "Because certain interconnected VoIP services can be used from virtually any Internet connection," the FCC explains, "the location of the caller cannot automatically be determined," including by emergency 911 operators.

[156] Cf. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

believed to be) abroad, the government need not follow FISA, even if the other party to the communication is in the United States, and even if the surveillance occurs on a wire or other facility in this country.[157]

This gives the government more power than it had in 1978, when FISA required a warrant for surveillance of international calls on wires located in the United States.[158] As discussed above (Part III), in 1978 the government legally could conduct such warrantless surveillance only by tapping wires abroad – *e.g.*, in Canada or the ocean. Perhaps there are good reasons for permitting such surveillance in the United States today. These may include technological or other operational issues associated with the use, location, or accessibility of fiber optic cables,[159] and the convenience (or perhaps necessity) of working with the assistance of telecommunications providers in the U.S., particularly as the volume and nature of international communications has expanded.[160] There may be other reasons appropriate for discussion in a closed session.

On the other side of the balance, it is worth considering whether concerns remain about warrantless surveillance of wires inside the United States. In 1978, as I understand it, those wires mainly carried domestic calls, while offshore wires carried international (or foreign-to-foreign) communications. Today, the situation is different, and the differences appear to be increasing. As General Hayden explained in 2006:

> A single communication can transit the world even if the communicants are only a few miles apart. And in that transit NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication … is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.[161]

Thus, warrantless wire surveillance in the United States of international calls (to or from the U.S.) may be more important, and could be less specially risky to domestic communications, than it was in 1978. An authoritative resolution of this issue is beyond

---

[157] 50 U.S.C. §§ 1805A, 1805B.

[158] See 50 U.S.C. § 1801(f)(2).

[159] As discussed above (Part II), the government has specifically identified the adoption of fiber optics as a technological problem for surveillance of international communications.

[160] Cf. discussion in text and note 130 (citing FISA Hearings 6-22-78 at 103, statement of H.W. William Caming, Attorney, AT&T, describing the relative lack of assistance provided to the government by AT&T in the 1970s). General Hayden has testified that "[t]he explosion of modern communications in terms of its volume, variety and velocity threatened to overwhelm" NSA beginning in the 1990s. Hayden Testimony 7-26-06. Today, FISA requires telecommunications providers to assist the government in national security wiretaps, 50 U.S.C. § 1805(c)(2), and the PAA's main provision applies only when a communications service provider or third party assists the government, 50 U.S.C. § 1805B(a)(3).

[161] Hayden Testimony 7-26-06 (emphasis added).

the scope of this paper, but it may be amenable to further consideration, at least in a closed session.[162]

C. Domestic Communications.

Although it apparently was not designed to permit surveillance of domestic communications, I believe the PAA may be read to accommodate such surveillance in certain circumstances. The argument in favor of that conclusion is relatively straightforward, and while there may be persuasive arguments against the conclusion, I have not seen them yet.

As amended by the PAA, FISA does not regulate surveillance "directed at a person reasonably believed to be located outside of the United States."[163] FISA defines a "person" to include "any individual … or any group, entity, association, corporation, or foreign power."[164] A "foreign power" is defined to include a "foreign government"; a "foreign-based political organization" and "a faction of a foreign nation" if they are not substantially composed of Americans; and a "group engaged in international terrorism."[165] Foreign governments and foreign-based political groups are (by definition) located abroad; factions of foreign nations are often located abroad; and international terrorist groups, such as al Qaeda, are almost always located abroad, even if they have individual members or affiliates inside the United States.[166] In any event, even if al Qaeda as a whole cannot be said to be located abroad, there is surely some "group" of international terrorists that is located abroad. Surveillance "directed at" such a group (or at any foreign power located abroad) is not regulated by FISA.

In the past, the government has taken the position that surveillance of a U.S. person's home and mobile telephones was "directed at" al Qaeda, not at the U.S. person himself.[167] Applied to the PAA, this logic would allow surveillance of Americans'

---

[162] A related issue, also worth consideration, is whether surveillance of domestic communications is now possible on wires located abroad, as discussed by Philip Lacovara in his testimony in 1976 and 1978.

[163] 50 U.S.C. § 1805A.

[164] 50 U.S.C. § 1801(m).

[165] 50 U.S.C. § 1801(a)(1), (2), (4), (5). A draft of the bill that became FISA referred to "foreign-based" terrorist groups, but the final version referred to "international" terrorist groups, both because "in the world of international terrorism a group often does not have a particular 'base,' or if it does, it may be nearly impossible to discern," and because "there are domestically based international terrorist groups" which Congress wanted to include in the definition. H.R. Rep. No. 95-1283, Part I at 30.

[166] For a discussion of these terms, and of the definition of "foreign power" in general, see *NSIP* Chapter 8.

[167] See *United States v. Bin Laden*, 126 F. Supp. 2d 264 (SDNY 2000). The court in *Bin Laden* rejected the government's position under the circumstances presented in the case. In other circumstances, however, the outcome might be different. More importantly, the decision in *Bin Laden* was that where surveillance is "directed at" both al Qaeda and an individual U.S. person, the government must satisfy the higher standards governing surveillance directed at the U.S. person. Under the PAA, where surveillance is directed at both al Qaeda (or another foreign power located abroad) and an individual U.S. person in the United States, the government could argue that 50 U.S.C. § 1805A still applies, and exempts the surveillance from FISA, because Section 1805A does not require surveillance to be "solely" directed at a person reasonably believed to be located outside the United States. For a more complete discussion of the *Bin Laden* case and related issues, see *NSIP* Chapter 16. For a discussion by two very smart observers of whether Section 1805A requires surveillance to be directed "solely" at a person located abroad,

telephones and e-mail accounts without a warrant, as long as the government could persuade itself that the surveillance was indeed "directed at" al Qaeda or another foreign power or group reasonably believed to be abroad.

More recently, the government has equated the PAA's "directed at" standard with FISA's traditional "targeting" standard,[168] meaning that surveillance under the PAA is "directed at" the person or entity from or about whom the government seeks information.[169] If that is correct, where surveillance seeks information from or about a foreign power that is (reasonably believed to be) located abroad, it may be conducted without adherence to FISA.

Under FISA, surveillance seeking information about (i.e., targeting) foreign powers often involves monitoring the communications of individuals.[170] That is because most foreign powers, like corporations, act (and communicate) only through their agents, as FISA's legislative history recognizes:

> Often, however, associations or entities will act or communicate in a "corporate" capacity, as distinguished from the acts or communications of an individual in the association or entity. For example, corporations lease phones, enter into contracts, communicate, and otherwise act as an entity distinct from the individuals therein. The fact that an individual officer or employee, acting in his official capacity, may sign the contract or communicate with a client on behalf of the corporation does not vitiate the fact that it is the corporation rather than the individual who is acting or communicating.[171]

The legislative history goes on to explain that FISA authorization orders targeting foreign powers may even involve a facility (*e.g.*, a telephone number) "dedicated to the use of one particular member of the entity," at least if the facility is "leased to or under the control of the entity."[172] The main requirement is that "the information sought must be concerning the entity, not the individual."[173]

---

see the dialogue between Marty Lederman and Orin Kerr, available at, *e.g.*, http://balkin.blogspot.com/2007/08/how-many-americans-might-be-under.html.

[168] See, *e.g.*, Wainstein Testimony 9-20-07 at 10.

[169] H.R. Rep. No. 95-1283, Part I at 73. For a more complete discussion of the term "target" and a comparison with the term "directed at," see *NSIP* Chapters 8 and 16. There is some language in the legislative history that might be read to suggest that surveillance is *per se* "directed at" the person or entity that owns or leases the facility being monitored, even if that person is not the surveillance "target." See H.R. Rep. No. 95-1283, Part I at 73-74; see also H.R. Rep. No. 95-1283, Part I at 31. I am not sure that is correct, and in any case the government appears to have adopted a different interpretation. If the government were to conclude that surveillance is *per se* "directed at" the person or entity that owns or leases a monitored facility, it might lead to problems in other possible applications of the PAA discussed below – *e.g.*, surveillance of generic facilities owned or leased by communications service providers in the United States.

[170] On the other hand, if surveillance "is to be directed at an individual about whom information is sought, that individual is the target and must be shown to be an 'agent of a foreign power,'" because individuals cannot themselves be "foreign powers" under FISA. H.R. Rep. No. 95-1283, Part I at 74.

[171] H.R. Rep. No. 95-1283, Part I at 74.

[172] H.R. Rep. No. 95-1283, Part I at 74.

Indeed, as explained elsewhere,[174] I believe the government has persuaded the FISA Court to authorize surveillance of international gateway switches, or other high-capacity facilities, under orders "targeting" al Qaeda and other terrorist groups. If that is correct, the same legal theory would apply to surveillance of domestic switches (or other domestic facilities), because the targets of the surveillance would remain the same. Ironically, surveillance of large, generic facilities like switches would be easier to accommodate under the PAA, because it would be harder to characterize as being "directed at" any particular individual located in the United States.[175]

The government unequivocally rejects the foregoing analysis. It maintains that the PAA "does not affect the application of FISA to persons inside the United States" because the plain language of the provision applies only to persons (reasonably believed to be) abroad. The government claims that the PAA "leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons in the United States." It goes on to discuss the language in 50 U.S.C. § 1805B authorizing collection of foreign intelligence information "concerning" persons outside the United States, and explains why the quest for such information is a necessary, but not sufficient condition for warrantless surveillance.[176] So far, at least, I am not persuaded by the government's legal position, in part because it does not come to grips with the specific arguments set out above,[177] although perhaps it may in time.

Legal arguments aside, the government has pledged unconditionally not to conduct warrantless surveillance of domestic communications under the PAA.[178] This is certainly within the government's discretion, but a discretionary decision by the executive branch may not satisfy many Americans. As one Senator stated in the debates on FISA, responding to the Attorney General's written promise that "it will be the policy and intent of the Department of Justice … to proceed exclusively by judicial warrant … against domestic communications of American citizens,"

> the "policy and intent" of the Justice Department is not enough. This legislation … should secure Americans from warrantless wiretapping in the United States *as*

---

[173] H.R. Rep. No. 95-1283, Part I at 74.

[174] *NSIP* Chapter 15.

[175] Of course, this analysis does not eliminate any Fourth Amendment limits on such surveillance, beyond the requirements of the statute itself.

[176] See Letter from Kenneth Wainstein, Assistant Attorney General, Department of Justice, to Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence at 2-3 (Sept. 14, 2007) [hereinafter Wainstein Letter 9-14-07].

[177] Those arguments were reviewed and cleared for publication by the Justice Department in the Slate Dialogue on August 28, 2007.

[178] See Wainstein Letter 9-14-07 at 3 ("To put it plainly: The Protect America Act does not authorize so-called 'domestic wiretapping' without a court order, and the Executive Branch will not use it for that purpose.").

a matter of federal law. If the legislation does not provide that protection, then it is defective.[179]

I believe it is unwise to have ambiguous national security legislation in this area. Such legislation leaves Intelligence Community personnel uncertain, civil libertarians anxious, and the executive branch open to after-the-fact criticism for having exercised too much self-restraint if we experience another major terrorist attack.

V. PENDING LEGISLATION

While this paper was undergoing prepublication review, two bills to replace the PAA were introduced in Congress. On October 12, 2007, the House Judiciary Committee reported the Responsible Surveillance that is Overseen, Reviewed and Effective (RESTORE) Act.[180] A few days later, the Senate Intelligence Committee approved the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007 (FAA).[181] The following paragraphs describe and analyze both bills at a relatively high level of generality. I begin with the FAA, because at this writing it seems much more likely than the RESTORE Act to serve as the vehicle for future legislation. More detailed analysis of both bills appears in an appendix.

A. The FAA.

Although the FAA is quite complex, its essential provisions can be summarized easily. It allows the government, "[n]otwithstanding any other law," to engage in the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information,"[182] with the acquisition not limited to any particular facility or place,[183] subject to three essential requirements:

- First, the acquisition "may be conducted only in accordance with" what are referred to in the bill as "targeting procedures,"[184] which must be "reasonably

[179] FISA Hearings 3-29-76 at 76 (statement of Senator Nelson) (italics in original).

[180] H.R. 3773; see H.R. Rep. No. 110-373 (Oct. 12, 2007).

[181] S. 2248; see S. Rep. No. 110-209 (Oct. 26, 2007) [hereinafter FAA Report]. This paper does not discuss the FAA's proposed Section 703(c) of FISA, concerning United States persons located abroad, because that provision is apparently still subject to a significant high-level policy dispute. The FAA would also substantially amend Subchapters I and II of FISA, and grant immunity to electronic communication service providers; this paper does not address those amendments.

[182] FAA Section 703(a). Section 101 of the FAA contains all of proposed subchapter VII of FISA, and this paper cites the proposed section numbers from within subchapter VII as if they were separate sections in the FAA. Other parts of the FAA are referred to by their section numbers within the FAA itself – e.g., FAA Section 102(a) refers to the proposed exclusivity provision in the bill.

[183] FAA Section 703(g)(3).

[184] FAA Section 703(d)(2).

designed to ensure that any acquisition … is limited to targeting persons reasonably believed to be located outside the United States."[185]

- Second, the acquisition "may be conducted only in accordance with" some version of traditional "minimization procedures,"[186] which must be "consistent with" the definition of that term applicable to electronic surveillance under Subchapter I of FISA.[187]

- Third, a senior Justice Department official and the Director of National Intelligence (DNI)[188] must certify in advance (or if necessary, within a week after acquisition begins),[189] that the targeting and minimization procedures satisfy the statutory requirements,[190] that a "significant purpose" of the acquisition is to obtain foreign intelligence information,[191] that the acquisition involves the assistance of an electronic communication service provider,[192] and that the acquisition is not "electronic surveillance,"[193] a term defined in Subchapter I of FISA and modified by the FAA to exclude "surveillance that is targeted in accordance with [the FAA] at a person reasonably believed to be located outside the United States."[194]

Under the FAA, the FISA Court reviews the targeting and minimization procedures to ensure that they meet the statutory requirements and the Fourth

---

[185] FAA Section 703(e)(1).

[186] FAA Section 703(d)(2).

[187] FAA Section 703(f)(1). The FAA uses "title" to refer to the various subchapters of FISA; for consistency with *NSIP*, this paper uses "subchapter."

[188] FAA Section 703(g); see FAA Section 702(a); 50 U.S.C. § 1801(g).

[189] FAA Section 703(g)(1)(A)-(B).

[190] FAA Section 703(g)(2)(A)(i) and (iv) (requiring attestation to the essential elements of FAA Sections 703(e) and (f)). The certification must also attest that the targeting procedures "are consistent with the requirements of the fourth amendments to the Constitution of the United States and do not permit the intentional targeting of any person who is known at the time of acquisition to be located in the United States." FAA Section 703(g)(2)(A)(ii). This requirement in the certification mirrors FAA Section 703(b)(1) and (3); there is no analogue in the certification to FAA Section 703(b)(2).

[191] FAA Section 703(g)(2)(A)(iii).

[192] FAA Section 703(g)(2)(A)(v). The term "electronic communication service provider" is defined in FAA Section 702(b)(4) to include telecommunications carriers as defined in the Communications Act (47 U.S.C. § 153), providers of electronic communications services as defined in Title III (18 U.S.C. § 2510), providers of remote computing services as defined in the Stored Communications Act (18 U.S.C. § 2711), "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored," and "an officer, employee, or agent of" these entities.

[193] FAA Section 703(g)(2)(A)(vi).

[194] FAA Section 701, modifying 50 U.S.C. § 1801(f).

Amendment,[195] and orders modifications if necessary; the court reviews the certification only as a matter of form, to ensure that it "contains all the required elements."[196] The court's order is issued to the government only – there is no provision in the bill for a secondary order. Instead, the government itself issues a "directive" to telecommunications providers requiring their assistance.[197] Providers may challenge such directives in the FISA Court,[198] and the government may seek FISA Court orders compelling compliance from a recalcitrant provider.[199] Thereafter, providers may be punished via contempt of court for noncompliance.[200] There are elaborate reporting and oversight procedures in the bill,[201] and a reiteration of FISA's 1978 "exclusivity provision."[202]

In my view, the FAA is an excellent vehicle for further legislative discussion and deliberation. It reflects a careful approach and substantial thought, and is in certain ways an improvement over the PAA. In particular, the FAA differs from the PAA in requiring the FISA Court to review (and approve or order modifications to) the targeting and minimization procedures governing surveillance of persons reasonably believed to be located outside the United States. According to media reports, the executive branch supports this approach, and believes it will not hinder essential operations. In this respect, therefore, the FAA is an improvement over the PAA, which did not require judicial review of minimization procedures.

My principal concern about the FAA, addressed in more detail in the appendix, is that it resembles the PAA in allowing surveillance of domestic communications. As

---

[195] See FAA Sections 703(e)(2) and (f)(2) (targeting and minimization procedures "shall be subject to judicial review"), 703(g)(2)(A)(i) and (iv) (certification must attest that targeting and minimization procedures "have been approved by, or will promptly be submitted for approval by, the Foreign Intelligence Surveillance Court"), 703(i)(1)(B) (requiring the Attorney General to transmit to the FISA Court the certification and targeting and minimization procedures and any directive of assistance issued to an electronic communication service provider within "5 days after making or amending the certification or determination or adopting or amending the procedures"), 703(g)(4) and (5) (requiring transmission of certification within "5 days after such certification is made" and providing for "judicial review" of the certification), 703(i) (providing that the FISA Court "shall have jurisdiction to review" the certification or targeting and minimization procedures), 703(i)(2)-(4) (providing that the FISA Court "shall review" the certification "to determine whether it contains all the required elements," and the targeting and minimization procedures to "assess whether" they meet the substance of the statutory requirements for those procedures).

[196] Under FAA Section 703(i)(5)(A), if "the Court finds that [the] certification … contains all of the required elements and that the targeting and minimization procedures … are consistent with the requirements of those subsections and with the fourth amendment … the Court shall enter an order approving the continued use of the procedures." If the Court does not so find, it "shall issue an order directing the Government to, at the Government's election," either "correct any deficiency" within 30 days, or "cease the acquisition." FAA Section 703(i)(5)(B).

[197] FAA Section 703(h).

[198] FAA Section 703(h)(4).

[199] FAA Section 703(h)(5).

[200] FAA Section 703(h)(5)(D).

[201] FAA Section 703(l).

[202] FAA Section 102(a); see 18 U.S.C. § 2511(2)(f) (current exclusivity provision, enacted in 1978 as part of FISA). For a more complete discussion of the current "exclusivity provision," see *NSIP* Chapter 15.

discussed in Part IV, there are situations in which surveillance may "target" a group, but still involve a facility used by an individual, as long as the government is trying to obtain information from or about the group. That possibility exists regardless of the location of the group and the individual. Thus, under the FAA as much as under the PAA, the government can (in some circumstances) conduct surveillance that "targets" (or is "directed at") al Qaeda, which is located outside the United States, on the telephone line or e-mail account of an American citizen located in the United States.

B. The RESTORE Act.

The RESTORE Act, now pending in the House of Representatives, is similar to the FAA, and has two main elements authorizing surveillance or related activity. First, it provides that "[n]otwithstanding any other provision of this Act, a court order is not required for the acquisition of the contents of any communication between persons that are not United States persons and are not located within the United States for the purpose of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States."[203]

This first provision is meant to permit warrantless surveillance of foreign-to-foreign communications, including e-mail messages that are stored on servers in the United States, where the parties involved are not Americans. This is well-intentioned, but it may not help the government very much. The chief problem here is the one identified in Part IV: the difficulty of determining the location of uncooperative parties to a communication. Added to that difficulty would be the RESTORE Act's omission of any "reasonably believed" modifier, suggesting that the government proceeds at its peril in determining whether a communication is indeed foreign-to-foreign. In addition, the provision does not apply to communications between Americans located abroad, which may make it intolerable to the government.[204]

In a second provision, the RESTORE Act provides that "electronic surveillance that is directed at the acquisition of the communications of a person that is reasonably believed to be located outside the United States and not a United States person for the purpose of collecting [certain types of] foreign intelligence information … by targeting that person shall be conducted pursuant to" either a court order, or an emergency authorization, issued under the new provisions of the bill.[205] This is meant to permit streamlined surveillance of international communications (with one end in the U.S.)

[203] RESTORE Act Section 2 (creating FISA Section 105A(a)).

[204] In that respect, the RESTORE Act is similar to Section 703(c) of the FAA.

[205] RESTORE Act Section 2 (creating FISA Section 105A(b)). The foreign intelligence information involved is "protective" information, defined by 50 U.S.C. § 1801(e)(1), and information relevant or necessary to "the national defense or security of the United States," 50 U.S.C. § 1801(e)(2)(A). The bill excludes information relevant or necessary to "the conduct of the foreign affairs of the United States," which is "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)(2)(B). For a more complete discussion of the term "foreign intelligence information." see *NSIP* Chapters 8 and 10.

when the target of the surveillance is a foreigner who is located abroad, even if the target is communicating with an American citizen in the United States.

To implement the authority granted in this second provision, the RESTORE Act provides for a FISA Court order, granting the government's application "as requested or as modified by the judge,"[206] to allow "acquisition of communications of persons that are reasonably believed to be located outside the United States and not United States persons … by targeting those persons."[207] The government's application must include (1) a certification from the DNI and the Attorney General that the targets are "reasonably believed" to be non-U.S. persons located abroad, and certain other factors;[208] (2) "procedures" that the FISA Court finds are "reasonably designed to determine" that the targets are non-U.S. persons located abroad;[209] (3) "minimization procedures" that the FISA Court finds meet the statutory definition of that term in Subchapter I of FISA governing electronic surveillance;[210] and (4) "guidelines" that the FISA Court finds are "reasonably designed to ensure" that an ordinary FISA application, under Subchapter I, will be filed whenever "a significant purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."[211]

The appendix contains a more detailed analysis of these provisions, but one preliminary concern is that the scope of the provisions is unclear. The RESTORE Act's

---

[206] RESTORE Act Section 3 (creating FISA Section 105B(e)(1)(A)).

[207] RESTORE Act Section 3 (creating FISA Section 105B(a)).

[208] RESTORE Act Section 3 (creating FISA Section 105B(b)(1)). In particular, the certification must state that (A) "the targets of the acquisition of foreign intelligence information … are persons reasonably believed to be located outside the United States," (B) the targets "are reasonably believed to be persons that are not United States persons," (C) the acquisition involves obtaining information "from, or with the assistance of, a communications service provider" or its agent, or from communications equipment used to "transmit or store such communications," and (D) a "significant purpose of the acquisition is to obtain" the designated subset of foreign intelligence information.

[209] RESTORE Act Section 3 (creating FISA Section 105B(b)(2)(A), (d)(1)). The application must include "a description of … the procedures that will be used by the Director of National Intelligence and the Attorney General during the duration of the [FISA Court] order to determine that there is a reasonable belief that the targets of the acquisition are persons that are located outside the United States and not United States persons." A judge of the FISA Court "shall approve the application if the judge finds that … the proposed procedures … are reasonably designed to determine whether the targets of the acquisition are located outside the United States and not United States persons." The application must also describe "the nature of the information sought, including the identity of any foreign power against whom the acquisition will be directed." RESTORE Act Section 3 (creating FISA Section 105B(b)(2)(B). This description is not reviewed by the FISA Court.

[210] The application must include a description of (A) "the procedures that will be used … to determine that there is a reasonable belief that the targets of the acquisition are persons that are located outside the United States and not United States persons," (B) "the nature of the information sought, including the identity of any foreign power against whom the acquisition will be directed," and (C) "minimization procedures" that satisfy the definition in 50 U.S.C. § 1801(h). RESTORE Act Section 3 (creating FISA Section 105B(b)(2)(A)-(C)). The FISA Court "shall approve" the government's application if it finds that the proposed procedures are "reasonably designed," and that the minimization procedures meet the statutory definition. RESTORE Act Section 3 (creating FISA Section 105B(d)(1)-(2)).

[211] RESTORE Act Section 3 (creating FISA Sections 105B(b)(2)(D) and 105B(d)(3)). To approve the application, the FISA Court must find that the guidelines are in fact "reasonably designed to ensure that an application is filed under [50 U.S.C. § 1804], if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."

authorization itself refers only to "electronic surveillance" that is directed at foreign persons abroad. But the provision implementing that authority refers more generally to court orders allowing "the acquisition of communications" of such persons, arguably not limited to "electronic surveillance." If the RESTORE Act is indeed limited to "electronic surveillance," rather than other forms of acquisition, I expect that the government will resist it, at a minimum because of the desire to conduct physical searches of stored communications.[212]

VI. CONCLUSION

This paper focused on the problem of determining the location of communicating parties, and the resulting consequences for FISA modernization. Despite the government's exaggerated historical claims, discussed in Part II, it is clear that (apart from the short-term amendments made by the PAA) FISA regulates more today than it did in 1978, at least with respect to surveillance of e-mail. As a practical matter, if not a legal one, the statute has expanded its scope, as explained in Part III. The expansion has created operational difficulties for the U.S. Intelligence Community, as explained in Part IV.

Those difficulties are in need of a legislative remedy. However, the current FISA amendments and bills – the PAA, the FAA, and the RESTORE Act – probably represent only interim solutions. That is because they continue to rely, at least to some degree, on the location of the FISA target. In our highly dynamic global communications environment, an interim solution may be the best we can do. In that spirit, Part V of the paper tried to identify how the FAA and RESTORE Act would function, and to suggest some possible improvements; the appendix contains more detailed analysis of both bills.

For the long run, however, we may need more radical change. This is true for at least three reasons. First, if the government genuinely cannot determine anything about a person's location, it makes no sense to use geography as a trigger for FISA's warrant requirements. In those circumstances, a geographical approach will always be too broad or too narrow – treating all communicating parties, or none, as if they were in the United States.

Second, I believe the government faces, and will continue to face, a similar problem with respect to determining nationality and identity, which are also triggers for FISA's warrant requirements. In 1978, a person's location gave rise to reasonable presumptions about his status as a United States person.[213] Today, even if location can be ascertained, the rise of global travel makes such a presumption far less defensible.

---

[212] See *NSIP* Chapter 7. References to "acquisition" in general, and to "stored" communications, see, *e.g.*, proposed FISA Sections 105B(a), (b)(1)(A)-(B), (b)(1)(C), suggest an intent to permit physical searches; references to "electronic surveillance" and to the minimization procedures governing electronic surveillance, see proposed FISA Section 105A(b), 105B(2)(C), suggest the opposite.

[213] For a discussion of this, see *NSIP* Chapter 9.

Third and finally, more and more human activities, from supermarket purchases to payment of highway tolls, leave permanent digital footprints. As a result, the coming years may yield an ever-expanding universe of communications and other information, which government (and the private sector) will want to acquire, but which may be very hard to process. The problem, in short, is that the vast and growing world of information may present in the form of what William James called a blooming, buzzing confusion. In more technical terms, the government may face a profusion of homogenized informational packets, devoid of reliable geographical order, subject to a growing divergence between physical location and communications location, and distorted by the use of various forms of virtual space, leaving nationality (and other attributes) of communicants largely indeterminate. In the future, if not today, the government may have access to more information about what is happening, but less ability to determine who is making it happen, where these persons are located, and why they are motivated to act as they do.

In light of these factors, and the remarkable changes the country has experienced in the past six years, we may need to undertake a broader effort to rationalize our national security law. At some point, Americans may be ready to pause, recapitulate, and reconsider these technological, operational, cultural, and legal developments systematically, not just in FISA, but in other areas. On the heels of efforts to describe the law governing national security investigations as it is,[214] it may soon be time to address the harder question of the law as it should be, based on everything we have learned before and since September 11, 2001.

[214] See, *e.g.*, *NSIP*.

Appendix: Detailed Comments on the FAA and the RESTORE Act

In the 1970s, when Congress was considering FISA, it held many hearings on draft legislation after the bills were reported by various committees of the House and Senate, with witnesses suggesting specific language in their testimony. The precise words used were subject to extensive review and comment over a long period of time. As of this writing, it appears that Congress does not intend to hold additional hearings on the FAA or the RESTORE Act. Accordingly, the comments below address in detail the language used in both bills.

I. COMMENTS ON THE FAA

A. Domestic Surveillance.

The FAA authorizes acquisition "targeting" persons (reasonably believed to be) abroad, and expressly prohibits the targeting of persons known to be in the United States.[215] As discussed in Part V, however, it does not foreclose all surveillance of domestic communications. That is because surveillance can "target" an international terrorist group located abroad, but still be directed at a domestic telephone number or other domestic communications facility. In this respect, the FAA resembles the PAA, as discussed in Part IV.[216]

The severity of this problem can be reduced with the following changes to the FAA:

- A new Section 703(b)(4): "shall not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States";

- New language immediately after "United States" in Sections 703(e)(1), 703(g)(2)(A)(i), and 703(i)(3): ", and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[217]

- New language in Sections 703(f), 703(g)(2)(A)(iv)(I), and 703(i)(4), adjusted to be grammatical in context: "The minimization procedures shall require the destruction, upon recognition, of any communication as to which the sender and all intended recipients are known to be located in the United States, a person has

[215] FAA Section 703(a)-(b).

[216] Indeed, the risk of this interpretation being adopted with respect to the FAA may be somewhat higher than it was for the PAA, at least if Congress is assumed to have been aware of concerns expressed about the PAA along these lines. See, *e.g.*, Slate Dialogue, Post # 6. On the other hand, as discussed below, Section 703(b) seems to represent an (imperfect) effort to prohibit domestic surveillance. See FAA Report at 14-15.

[217] Corresponding language could also be added to Section 703(g)(2)(A)(ii) if desired, and if that subsection remains in the bill.

a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes, unless the Attorney General determines that the communication indicates a threat of death or serious bodily harm to any person."[218]

These changes are imperfect because, as explained in Part IV, location is difficult to determine in the modern world of communications, and the restrictions apply only when the government "knows" that the communication is domestic.[219] But the changes should help prevent surveillance of domestic communications made on Americans' telephones, e-mail accounts, and other communications facilities. At a minimum, for example, surveillance of a wireline telephone number in New York City would be possible only with respect to international calls, not domestic calls, made from the number,[220] and surveillance of domestic e-mail messages to or from an ISP in the United States also would not be possible.[221]

B. Domestic Targeting Limits in FAA Section 703(b).

Section 703(b) of the FAA attempts to limit the acquisition authority, granted in Section 703(a), to the targeting of persons reasonably believed to be abroad. It provides that the acquisition (1) "may not intentionally target any person known at the time of the acquisition to be located in the United States"; (2) "may not intentionally target a person reasonably believed to be outside the United States if the purpose of such acquisition is to target for surveillance a particular, known person reasonably believed to be in the United States, except in accordance with" Subchapter I of FISA; and (3) "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."

[218] This language is modeled on 50 U.S.C. § 1806(i), which applies to unintentionally acquired radio communications under Subchapter I of FISA. Section 1806(i) was designed to guard against the "potential for abuse if the Government acquired those kinds of domestic communications, even without intentionally targeting any particular communication" – i.e., through vacuum-cleaner surveillance as described in Part III. H.R. Rep. No. 95-1283, Part I at 94. Section 106 of the FAA amends 50 U.S.C. § 1806(i) to cover all communications, not merely radio communications, but limits it to "unintentionally" acquired communications. As discussed below, in the analysis of FAA Section 703(b), this has the potential to suggest that "intentionally" acquired domestic communications are exempt from the destruction requirement. In any event, it seems appropriate to include a destruction requirement for domestic communications in the minimization procedures for new Subchapter VII itself, rather than in the use provisions of Subchapter I.

[219] A lower standard, such as "reasonably believes," may be worth exploring, but probably will prove to be unworkable. Cf. S. Rep. No. 95-701 at 36 ("Only 'intentional' acquisitions of private domestic radio communications are within [50 U.S.C. § 1801(f)(3)] because, 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. Thus, intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of communications intended to be totally domestic.").

[220] In theory, at least, it is conceivable that the government could conduct surveillance on a domestic wireline telephone number, configuring the surveillance equipment with the aid of a pen register to record communications only when an international access code (e.g., 011 for all international calls from the U.S., or 011-93 for calls from the U.S. to Afghanistan) is dialed. Perhaps the same could be done for incoming international calls using a trap-and-trace device.

[221] There may be other ways to remedy the problem of domestic surveillance, but I am not sure they can be discussed in an unclassified setting.

As noted above, by focusing on "targets," rather than "communications," Section 703(b) will not prevent all domestic surveillance. Moreover, while it seems well-intentioned, Section 703(b) may ultimately do more harm than good because of the way it is drafted. As a result, I believe it should be removed, amended, or clarified, as detailed in the analysis of its three subsections below.[222]

Section 703(b)(1)

The main problem with Section 703(b)(1) is that it appears redundant, and therefore may provoke unintended interpretations. On its face, Section 703(b)(1) adds nothing to the FAA: surveillance that satisfies the baseline requirement of Section 703(a) – because it involves "the targeting of persons reasonably believed to be located outside the United States" – cannot possibly "target any person known … to be located in the United States" within the meaning of Section 703(b)(1).[223] As a result, under settled principles of statutory construction,[224] courts will reach for alternative interpretations of Section 703(b)(1) that give it independent effect.

One alternative is to read Section 703(b)(1) to change the law by assuming the possibility of multiple FISA targets for a single act of surveillance.[225] This approach would give Section 703(b)(1) real meaning, because it would then serve to prohibit what would otherwise be permitted – targeting a person abroad while also targeting a (different) person in the U.S. The cost, however, would be implicitly to authorize multiple targets where the prohibition of Section 703(b)(1) does not apply – *e.g.*, in Subchapter I of FISA. That would be a significant change, should be considered carefully before being enacted, and if enacted should be in the form of an explicit definition of the term "target" rather than a purported limit on domestic surveillance.

Section 703(b)(2)

Section 703(b)(2) also appears redundant. Given the baseline requirement for foreign targeting under Section 703(a) as described above, courts will strain to find independent meaning in the requirement that the government not have a "purpose … to

[222] The analysis that follows is not meant to suggest the best possible interpretation of Section 703(b), but only to identify the risk of possible misinterpretations while the provision is still subject to revision. That risk can be mitigated in a variety of ways other than by editing or removing Section 703(b), including adding explanatory legislative history. Even if Section 703(b) becomes law, I do not think it should be read as described in this paper; I merely worry that it might be.

[223] Perhaps Section 703(b)(1) can be saved from redundancy by being treated as a clarification that "belief" cannot be "reasonable" when contradicted by actual "knowledge."

[224] See, *e.g.*, *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253 (1992) ("courts should disfavor interpretations of statutes that render language superfluous").

[225] Traditionally, FISA has been understood to involve only a single target. See H.R. Rep. No. 95-1283, Part I at 73-74 (describing the FISA target as the person or entity from or about whom the government seeks information). For a more complete discussion of "target" as used in FISA, see *NSIP* Chapter 8. In *United States v. Bin Laden*, 126 F. Supp.2d 264 (2000), the district court appears to have concluded that surveillance can be "directed at" multiple persons or entities within the meaning of Section 2.5 of Executive Order 12333. For a more complete discussion of Section 2.5 and the *Bin Laden* decision, see *NSIP* Chapter 16.

target for surveillance a particular, known person reasonably believed to be in the United States, except in accordance with title I" of FISA. Several possibilities, none of them benign, present themselves.

First, as noted above, Section 703(b)(2) may suggest the validity of multiple FISA targets in situations where it does not apply. This would give the provision independent meaning, at least when compared to Section 703(a), although its interaction with Section 703(b)(1) would remain to be determined.

Second, by referring to targeting for "surveillance … except in accordance with" Subchapter I of FISA, Section 703(b)(2) could suggest by negative implication that the government may engage in acquisition activity that is not "surveillance," and not conducted "in accordance with" Subchapter I, such as a physical search.[226] In other words, Section 703(b)(2) may be read to allow the government to intentionally target a person abroad, even if the purpose of the acquisition is to target for search (rather than surveillance) a particular, known person in the United States.

Third, by referring to targeting "a particular, known person," Section 703(b)(2) may suggest by negative implication that the government may engage in acquisition if the "purpose of such acquisition is to target for surveillance" all persons, rather than a "particular, known person," reasonably believed to be in the United States.[227] The reference to a "particular, known" person comes from the current definition of "electronic surveillance";[228] as discussed in Part III, the definition was designed to permit "vacuum-cleaner" surveillance of all communications on a particular channel, as long as the surveillance did not target particular Americans in the United States (*e.g.*, by using their names as watchlist selectors). Thus, Section 703(b)(2) may be read to allow the government to intentionally target a person abroad, even if the purpose of the acquisition is to target everyone (but not anyone in particular) in the United States.[229]

---

[226] This is especially possible when the provision is read in contrast to Section 703(b)(1), which does not distinguish between "surveillance" and other methods of acquisition or targeting.

[227] Again, the contrast with Section 703(b)(1), which does not refer to "particular, known" persons, contributes to this possibility.

[228] Under 50 U.S.C. § 1801(f)(1), "electronic surveillance" is defined to include "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

[229] It is also possible to read "particular, known" persons in Section 703(b)(2) as recognizing that surveillance of a person abroad will inevitably acquire the communications of all of his interlocutors in the United States, and as permitting such acquisition unless those interlocutors become the persons from or about whom the government is (primarily) seeking information. In other words, it is possible to read Section 703(b)(2) as emphasizing the prohibition on "reverse targeting," under which the nominal target is Smith, but the government's real purpose is to acquire information from or about Jones, who communicates with Smith. Indeed, I assume that this is the purpose of Section 703(b)(2), as the FAA Report (at pages 14-15) seems to say. But this limitation is already part of the general law of "targeting" under FISA, see H.R. Rep. No. 95-1283, Part I at 50 n.25, 73-74; S. Rep. No. 95-701 at 51; S. Rep. No. 95-604 at 45, and so courts may strain for alternative interpretations.

Fourth, the use of "intentionally" to modify "targeting" probably should be avoided,[230] because targeting is inherently an intentional act under FISA. To be sure, the current definition of "electronic surveillance" refers to "intentional" targeting.[231] As discussed in Part III, however, "intentional" in the current definition reflects the special problem of non-targeted SIGINT; indeed, "intentionally" is probably redundant even in that context. In any event, the use of "intentionally" in Section 703(b)(2) is particularly strange, because it modifies the targeting of the person abroad, not the person in the United States. In other words, if "intentional" means anything as used in Section 703(b)(2), it seems to leave room for unintentional targeting of persons abroad, even if the government is also (intentionally) targeting a particular, known person in the United States.

Section 703(b)(3)

Section 703(b)(3) is unobjectionable, insofar as the Fourth Amendment applies regardless of the statute, and may serve to emphasize that the "manner" of "conduct[ing]" the surveillance, as well as the scope of the surveillance, must satisfy constitutional limits.[232] Indeed, Section 703(b)(3) supports the idea that Sections 703(b)(1)-(2) also merely emphasize otherwise-applicable rules, and do not intend to radically revise existing understandings of FISA.

C. Acquisition Other than Electronic Surveillance.

By authorizing "the targeting of persons" outside the United States[233] in accordance with procedures governing the "acquisition" of information from that targeting,[234] and by requiring that the "acquisition … not constitute electronic surveillance"[235] as that term is defined by Section 701, the FAA seems to permit not only surveillance activities, but also any other method of targeting and acquiring foreign intelligence information from or about a person (reasonably believed to be) located abroad. Examples include physical searches, and perhaps requests to third parties for documents and other tangible things. The government may well need to engage in physical searches of stored electronic communications or other data,[236] but depending on its policy preferences, Congress may want expressly to forbid certain other physical searches (*e.g.*, of a U.S. person's home), searches of the U.S. mail, and perhaps

[230] The word "intentionally" also appears in Section 703(b)(1).

[231] 50 U.S.C. § 1801(f)(1).

[232] See, *e.g.*, *United States v. Ramirez*, 523 U.S. 65 (1998).

[233] FAA Section 703(a).

[234] FAA Section 703(e), (f).

[235] FAA Section 703(g)(2)(vi).

[236] For an explanation of why this is so, see *NISP* Chapter 7.

collection of transactional records pertaining to communications.[237] This could be done by adding limiting language to the FAA as explained in the discussion of domestic surveillance above.[238] Alternatively, Congress may prefer to identify the collection techniques that are authorized under the bill, rather than those that are not authorized. This has the added advantage of making clear that the alternative collection techniques – *e.g.*, physical searches of stored data – are indeed permitted where appropriate.

D. Exclusivity Provision.

The exclusivity provision in Section 102(a) of the FAA is problematic because of its intersection with the current exclusivity provision,[239] and perhaps because of its failure to reference Chapter 206 of Title 18 (concerning criminal pen-trap surveillance) and Rule 41 of the Federal Rules of Criminal Procedure (concerning silent video surveillance). Here, the remedy may vary according to Congress's policy goals.

If the goal of Section 102(a) is simply to retain the operative effect of the exclusivity provision, despite the FAA's limit on the definition of "electronic surveillance," then it would be better to amend the existing exclusivity provision than to enact a new provision without repealing the old one. The amendment would be to add the phrase "(regardless of the limitation of section 701 of such Act)" immediately after "as defined in section 101 of such Act" in the existing exclusivity provision.[240]

If the goal of Section 102 is also to disapprove the pre-judicial version of the Terrorist Surveillance Program (TSP) and other assertions of Presidential authority in this area, then explanatory legislative history accompanying the amendment (or perhaps even a joint resolution) may be the better course. The explanation in the FAA Report, taken from the original Conference Report on FISA, is an effective general statement of this sort, making clear (by citing the *Steel Seizure* case[241]) that Congress intends to "place any power of the President to disregard [the exclusivity provision] 'at the lowest ebb.'"[242] If Congress wishes to go further, it also could address the specific arguments advanced by the executive branch in support of the TSP, including the

[237] The concern here with respect to the FAA is less than it was with respect to the PAA, because the FAA requires a certification (albeit reviewed only for form) that the acquisition "involves obtaining the foreign intelligence information from or with the assistance of an electronic communication service provider," (Section 703(g)(2)(A)(v); see also FAA Section 702(b)(4)), while the PAA allowed acquisition with the assistance of "any person" who had access to communications while being transmitted or stored (50 U.S.C. § 1805B(a)(3)). This reference to "any person" in the PAA raised speculation that the government might use the statute to conduct a physical search of an apartment with the assistance of a landlord who had access to the computer or U.S. mail located within.

[238] The amendments would be included in FAA Sections 703(b)(4), 703(e)(1), 703(g)(2)(A)(i), and 703(i)(3).

[239] 18 U.S.C. § 2511(2)(f).

[240] 18 U.S.C. § 2511(2)(f).

[241] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

[242] FAA Report at 18 (citing H.R. Conf. Rep. No. 95-1720 at 35 (1978), and quoting *Youngstown,* 343 U.S. at 637 (Jackson, J., concurring)).

claims that FISA incorporates all other possible surveillance statutes via its criminal penalty provision,[243] and that the exclusivity provision and these statutes must be read to permit the TSP under the doctrine of constitutional avoidance.[244] A resolution or legislative history also would avoid any uncertainty about the meaning of a new exclusivity provision while the old one, with its slightly different language, is still on the books.

If Congress legislates concerning the exclusivity provision, it probably should add explicit references to Chapter 206 of Title 18, and Rule 41 of the Federal Rules of Criminal Procedure, to remove any uncertainty about the continuing validity of pen-trap surveillance and silent video surveillance in ordinary criminal investigations. Those references are needed because pen-trap surveillance and silent video surveillance are "electronic surveillance" as defined by FISA,[245] but neither is authorized in ordinary criminal investigations by FISA or any of the other laws mentioned in the current or proposed exclusivity provision.[246] As a result, defendants have argued that silent video surveillance is forbidden by the exclusivity provision in ordinary criminal investigations. The courts of appeals have rejected that argument by holding "that the Foreign Intelligence Surveillance Act is intended to be exclusive in its domain and Title III in its," so that FISA has no preclusive effect in ordinary criminal cases.[247] The logic of those holdings would likely survive enactment of the FAA, but it may make sense to remove any uncertainty.

E. Definition of "Electronic Surveillance".

Section 701 of the FAA limits the definition of "electronic surveillance" as follows: "Nothing in the definition of electronic surveillance under [50 U.S.C. § 1801(f)] shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States." This provision, and its cognate in Section 703(g)(2)(A)(vi), can safely be removed from the bill.

Section 701 does not give the government any additional authority to conduct appropriate surveillance. The FAA already authorizes acquisition "[n]otwithstanding any other law," which means that it will fulfill its function even if the current definition of "electronic surveillance" remains intact. To eliminate any doubt on the issue, clarifying language could (and probably should) be added along the lines of FISA's pen-trap provisions, providing that the authority in new Subchapter VII of FISA is "in addition to"

---

[243] 50 U.S.C. § 1809.

[244] For a more complete discussion of the government's specific statutory and constitutional arguments in favor of the TSP, and arguments in response, see *NSIP* Chapter 15.

[245] See 50 U.S.C. §§ 1801(f), 1801(n). For a more complete discussion of this issue, see *NSIP* Chapters 7 and 17.

[246] Criminal pen-trap surveillance is authorized by Chapter 206 of Title 18, and criminal silent video surveillance is authorized by Federal Rule of Criminal Procedure 41.

[247] *United States v. Torres*, 751 F.2d 875, 881 (7th Cir. 1985); see *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994) (citing cases). For a more complete discussion of these cases and this issue, see *NSIP* Chapter 15.

the authority under the other subchapters.[248] With that language (or even without it), the FAA will authorize acquisition from targets located abroad regardless of Section 701.

Nor does Section 701 protect the government in other ways. To be sure, treating FAA acquisition as "electronic surveillance" means that it will be subject to FISA's criminal and civil penalty provisions.[249] Even from the government's perspective, however, this should not be a problem. The penalty provisions apply only to surveillance not "authorized by statute," which means that acquisition in accordance with the FAA is immune without regard to Section 701.[250] On the other hand, Section 701 itself cabins the definition of "electronic surveillance" only with respect to acquisition "targeted in accordance with this title." Thus, it does not exempt acquisition conducted in violation of the FAA: acquisition that violates the FAA's targeting rules is "electronic surveillance," even if the target is abroad.[251] In short, acquisition "targeted in accordance with" the FAA cannot violate FISA's penalty provisions even without Section 701 in the bill, and electronic surveillance not "targeted in accordance with" the FAA may violate them even with Section 701 in the bill.[252]

F. Miscellaneous Comments.

In addition to the policy issues discussed above, there are several technical and drafting issues with the FAA worth considering:

- In Section 703(i)(1)(A), the "or" probably should be changed to "and."

- If Section 703(b) is removed from the bill, Section 703(g)(2)(A)(ii) also may be removed. On the other hand, if Sections 703(b) and 703(g)(2)(A)(ii) remain in the

[248] 50 U.S.C. § 1842(a)(2). As discussed in *NSIP* Chapter 17, pen-trap surveillance is "electronic surveillance" under FISA, but the authority to conduct pen-trap surveillance, a special and limited form of "electronic surveillance," is granted by Subchapter III of FISA "in addition to" the broader authority in Subchapter I.

[249] 50 U.S.C. §§ 1809 and 1810.

[250] As discussed in *NSIP* Chapter 14, these provisions forbid only willful violations, requiring not only an intentional act, but one that the actor knows to be illegal.

[251] As the FAA Report explains (page 14), "the limitation on the Title I definition of electronic surveillance is no broader than the authority under Title VII for electronic surveillance targeted at persons reasonably believed to be outside the United States." There is, of course, some ambiguity about the phrase "targeted in accordance with this title" in Section 701, although I do not think the ambiguity is fatal. Is surveillance that violates the targeting procedures "electronic surveillance" even if the target is reasonably believed to be abroad, and is in fact abroad? Perhaps courts would not treat every inadvertent violation of the targeting procedures as a failure to "target[] in accordance with this title," and therefore as "electronic surveillance," but they probably would do so for intentional or reckless disregard of the targeting procedures, especially on a broad scale, and (as noted above) FISA's penalty provisions apply only to willful violations. Surveillance conducted in violation of the FAA's minimization procedures probably would not be "electronic surveillance," unless the minimization procedures could be said to govern "targeting."

[252] Under FAA Section 704, acquisition under the FAA is already treated as "electronic surveillance" for purposes of FISA's notice, use, and disclosure provisions. See 50 U.S.C. § 1806. For a discussion of this part of the statute, see *NSIP* Chapters 26-30.

bill, perhaps an analogue to Section 703(b)(2) should be added to Section 703(g).

- There is no explicit contempt authority where the FISA Court denies a petition submitted by a provider, as there is when the government seeks a compliance order. Section 703(h)(5). Inherent authority should suffice, however.

- The bill provides that the certification "is not required to identify the specific facilities, places, premises, or property at which the acquisition … will be directed or conducted."[253] This may be an important part of the bill, but it probably should be stated with respect to the targeting procedures, not the certification.

- It is worth considering whether the Attorney General himself, rather than the "Attorney General" as defined by Section 702(a),[254] should have to approve the procedures and issue the certification. It is a little asymmetrical, though certainly not improper, to have the DNI issuing a certification with an Assistant Attorney General.

- By authorizing "acquisition" that targets persons abroad, the FAA apparently contemplates not only electronic surveillance, but also physical searches and other methods of collection, as discussed above. Yet the "minimization procedures" required by the FAA are solely those applicable to electronic surveillance,[255] not those applicable to physical searches.[256] References in the FAA to minimization procedures that are "consistent with the requirements of section 101(h)" could be changed so they refer to minimization procedures that are "consistent with the requirements of sections 101(h) or 121(4), as appropriate," and could also refer to minimization consistent with the requirements of section 161(g), if compelled production of tangible things is to be authorized.

II. COMMENTS ON THE RESTORE ACT

I have only a few supplemental observations on the RESTORE Act, focused on what I believe is its main distinguishing feature – a requirement that the government proceed under Subchapter I of FISA "when a significant purpose of an acquisition" targeting a foreign person abroad "is to acquire the communications of a specific person reasonably believed to be located in the United States."[257] Like Section 703(b) of the FAA, discussed above, this provision aims generally to prevent some version of reverse

[253] FAA Section 703(g)(2)(3).

[254] See 50 U.S.C. § 1801(g).

[255] 50 U.S.C. § 1801(h).

[256] 50 U.S.C. § 1821(4).

[257] RESTORE Act Section 105B(b)(2)(D).

targeting, under which the nominal target is Smith (a foreign person abroad), but the government's real purpose is to acquire information from or about Jones (a person in the U.S.), who communicates with Smith.

Unlike FAA Section 703(b), the RESTORE Act does not necessarily assume or suggest the possibility of two FISA targets. That is because a "significant purpose" to acquire information from or about Jones would not necessarily make him a FISA target, as long as the government's "primary purpose" remained the acquisition of information from or about Smith. To be sure, the law of targeting has not generally been described in terms of primary or significant purpose – FISA contains no definition of the term – but there is nothing in the legislative history to suggest that the government must have an "exclusive" purpose to acquire information from or about its target. If targeting is to be described in terms of purpose, the sensible conclusion is that the identity of the target depends on the government's "primary" purpose.[258] The RESTORE Act seems consistent with that.

Even with a primary purpose to target a person abroad, however, the RESTORE Act requires the government to proceed under Subchapter I when it develops a "significant purpose" to acquire information from or about a person in the United States. That significant purpose does not change the identity of the FISA target; it simply triggers the obligation to proceed under Subchapter I despite the fact that the target is a foreign person located abroad.

Although consistent with traditional targeting law, I believe the RESTORE Act's "significant purpose" standard will prove unworkable. Congress has some familiarity with the "significant purpose" standard, having enacted it in Section 218 of the USA PATRIOT Act,[259] requiring the government to have a "significant purpose," rather than a "primary purpose," to obtain foreign intelligence information. Indeed, Congress saw the "significant purpose" standard interpreted by the Foreign Intelligence Surveillance Court of Review,[260] and subsequently reaffirmed the standard in reauthorizing the Patriot Act.[261] Thus, the Court of Review's interpretation of "significant purpose" with respect to foreign intelligence information will likely influence any future interpretation of "significant purpose" with respect to targeting.

The Court of Review held that the "significant purpose" test is easily satisfied:

> So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.

---

[258] See H.R. Rep. No. 95-1283 Part I at 73-74.

[259] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. 107-56, 115 Stat. 272 (Oct. 25, 2001); see 50 U.S.C. § 1804(a)(7)(B). For a discussion of the history leading up to enactment of Section 218, see *NSIP* Chapter 10.

[260] *In re Sealed Case*, 310 F.3d 717 (2002).

[261] See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102(a), 120 Stat. 192, 194 (2006).

> The important point is … the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution – such as stopping an ongoing conspiracy –
> and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct … to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.[262]

Under this version of "significant purpose," as applied to the RESTORE Act, the government would have to proceed under Subchapter I whenever it had a "realistic" interest in Jones, the person in the United States, even if it also had an overwhelming interest in Smith, the foreign person abroad. That standard is too low to function in this context, and might also create serious administrative difficulties, forcing the government continually to determine and document whether it had developed any "significant" interest in the various Joneses with whom its targeted Smiths may communicate over time.

Moreover, I am not sure what would happen under the RESTORE Act if a Subchapter I application on Jones were denied. Would the government then have to stop surveillance on Smith? If it is not the case, there seems little point in requiring the application on Jones in the first place. If it is the case, however, the government could lose coverage on Smith, regardless of his significance, where it also had a significant interest in Jones, if it lacked the information necessary to establish probable cause that Jones is the agent of a foreign power.

[262] 310 F.3d at 735.