Statement for the Record
K. A. Taipale, Executive Director
Center for Advanced Studies in Science & Technology Policy

Foreign Intelligence Surveillance Modernization: Reconciling Signals Intelligence Activity with Targeted Wiretapping

Senate Select Committee on Intelligence Hearing on
The Foreign Intelligence Surveillance Modernization Act of 2007

May 1, 2007

The Center for Advanced Studies in Science and Technology Policy, an independent, non-partisan research organization focused on information, technology, and national security policy, has long advocated that the Foreign Intelligence Surveillance Act of 1978 ("FISA") be carefully amended to provide an updated statutory mechanism so that legitimate foreign intelligence and national security needs can be met while still protecting privacy and civil liberties. [1]

On April 13, 2007 the Director of National Intelligence submitted legislation to Congress (Title IV of the Fiscal Year 2008 Intelligence Authorization Act, The Foreign Intelligence Surveillance Modernization Act of 2007) ("FISMA") requesting that FISA be amended "to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the United States."

We are pleased to submit this statement discussing certain issues relating to FISA modernization in connection with the Senate Select Committee on Intelligence hearing to consider this legislation. We focus in this statement primarily on the issues relating to the use of signals intelligence activities, including those targeted against legitimate foreign intelligence targets not subject to FISA, when those activities may have significant impact on U.S. persons because they involve communications to or from the United States.

---

[1] *See, e.g.,* K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance,* N.Y.U. REV. L. & SECURITY, NO. VII SUPL. BULL. ON L. & SEC.: THE NSA AND THE WAR ON TERROR (Spring 2006) at *http://whisperingwires.info/*; and K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128 *(Spring 2007) available at* http://ssrn.com/abstract=959927.

Introduction.

FISA should be amended as it is no longer adequate either to enable legitimate foreign intelligence activity or to protect privacy and civil liberties. FISA simply did not anticipate the nature of the current threat to national security from transnational terrorism, nor did it anticipate the development of global communication networks or advanced technical methods for intelligence gathering. Because of technology developments unanticipated in 1978, FISA warrant and procedural requirements are now being triggered in circumstances not originally intended to be covered by FISA and for which such procedures were not designed and are not well-suited. [2]

The current public debate over FISA modernization is needlessly polarized because of a failure to adequately address directly the fundamental political and policy challenges resulting from this blurring of the previously clear demarcation between reactive law enforcement-derived policies governing the use of targeted "wiretaps" to monitor communications of known persons in the United States pursuant to warrants issued on a prior showing of probable cause on the one hand, and preemptive national security strategies that rely on "signals intelligence" (activity not directed at targeted individuals in the United States but rather at finding information with foreign intelligence value for counterterrorism or counter-proliferation purposes from monitoring foreign intelligence channels or targets, including their international communications to and from the United States) to identify and preempt unknown threats on the other.

As discussed in the following section, when FISA was enacted it was intended only to cover targeted domestic surveillance for foreign intelligence purposes. In keeping with this intent, the administration has proposed amending FISA to exclude non-targeted signals intelligence activity from the definition of "electronic surveillance." In addition, the Attorney General would be given authority to approve "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside of the United States" from "communication service providers" (provided that such acquisition did not constitute the newly defined "electronic surveillance").

The effect of these changes would be to exclude from FISA warrant requirements foreign signals intelligence activities directed at legitimate foreign intelligence targets outside of the United States, including their communications to and from the United States, and, if authorized by the Attorney General, additional foreign intelligence information relating to these targets obtained from domestic communication providers. Information obtained through these activities that concerned U.S. persons would be subject to minimization procedures but would be available for use to support FISA warrant applications to target such U.S. persons if the information had significant foreign intelligence value.

---

[2] See generally, *id*.

We have previously advocated that FISA be amended (1) to provide an explicit statutory authorization and oversight mechanism for programmatically approving certain foreign signal intelligence activity that may substantially affect U.S. persons, and (2) to provide an explicit procedure for using information derived from such signals intelligence activity as a predicate in appropriate cases for subsequent targeted "wiretap" surveillance pursuant to FISA warrant procedures.

While the administration's proposed amendments address the same problems with FISA that we have previously identified—and we generally support the effort to modernize FISA—we would prefer to see an additional statutory authorization or oversight mechanism specifically designed to provide additional privacy and civil liberties protection (through specific authorities, oversight, or review) for situations in which either programmatic or foreign-targeted signals intelligence activities are likely to have a significant impact on persons in the United States. Thus, we urge that the Committee, the Congress, and the administration consider the issues discussed below.

Changes in technology challenge the existing FISA framework.

When FISA was enacted in 1978 it was intended only to cover targeted foreign intelligence interceptions of domestic communications within the United States. It was specifically not intended to cover non-targeted signals intelligence activities to collect foreign intelligence (nor communications intercepted incidental to surveillance targeting a foreign intelligence target not itself subject to FISA). The exclusion of National Security Agency ("NSA") signals intelligence activities, including activities directed at intercepting international communications, was explicitly acknowledged at the time:

> Because of the different nature of government operations to collect foreign intelligence by intercepting international communications—a process described as the interception of signals and the processing of those signals by techniques which sort and analyze the signals to reject those that are inappropriate or unnecessary—that use of electronic surveillance is not addressed in this bill. [3]

The legislative history is replete with references acknowledging Congressional awareness of ongoing signals intelligence activities relating to international communications then being conducted by the NSA (including "sweeping" interceptions of communications where one end was in the United States) and makes it clear that it was not contemplated that such activity was to be subject to FISA warrant or procedural requirements. [4]

---

[3] *Foreign Intelligence Surveillance Act, Hearing before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, United States Senate*, 94th Congress, at 11 (March 29-30, 1976) (Statement of the Hon. Edward H. Levi, Attorney General of the United States).

[4] For example, Attorney General Levi testified that "[w]here there is a radio communication [including the microwave portion of a wire transmission, *see* note 5 *infra*] of an international kind which is picked up in some kind of sweeping operation or some other kind of operation; that is beyond the scope of [FISA]." Statement, *supra* note 3 at 15. And further, "I think the fact of the matter is that this bill does not provide for facts and circumstances, which I specifically mentioned, namely the transatlantic kinds of sweeping overhearing, with which members of this committee, I am sure, are somewhat familiar. *Id.* at 17.

Indeed, the differing statutory standards enacted in FISA for "wire" and "radio" intercepts, and for interceptions conducted "within the United States" and abroad, were designed specifically as statutory mechanisms to preserve the distinction between signals intelligence not subject to FISA and targeted domestic activity that was to be its domain.[5]

Thirty years ago when FISA was being drafted these technical distinctions based on place or method served to distinguish signals intelligence from targeted "wiretapping" and made perfect sense given the then prevalent practices and technologies. Signals intelligence activities at that time were primarily being conducted by foreign intelligence agencies like the NSA through interception of satellite or microwave transmissions (i.e., "radio") that could be intercepted from abroad (even when they had one "end" in the United States), and targeted interceptions of specific communications of known persons were generally being conducted by law enforcement or counterintelligence agencies like the FBI using a "wiretap or microphone" on circuit-based "wire" transmissions within the United States. FISA was intended to cover the latter and designed to exclude the former.[6]

And, at a subsequent FISA hearing in the House, when asked by Congressman Railsback to give a specific example of an activity that was not within the scope of FISA, the Attorney General stated: "… 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." *Foreign Intelligence Surveillance Act, House Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary*, 94th Congress, at 91 (June 2, 1976) (Statement of Edward H. Levi, Attorney General of the United States).

[5] This intention is explicitly acknowledged in the legislative history:

> The reason for excepting from the definition of "electronic surveillance" the acquisition of international radio transmissions, including international wire communications [i.e., international telephone calls] when acquired by intercepting radio transmission [i.e., microwave transmission thereof] when not accomplished by targeting a particular United States person in the United States, is to exempt from the procedures of the bill certain signals intelligence activities of the National Security Agency.

S. REP. NO. 95-604, 95th Cong., at 34 (1977).

The intentionality of this distinction between "wiretap" activities and signals intelligence activities is further evidenced by the way FISA explicitly defines "wire transmission" as "any communication *while it is being carried by a wire, cable, or other like connection*" (50 U.S.C. §1801(l), emphasis added). This qualifier—"*while it is carried by*"— is necessary because 18 U.S.C. §2510(1) defines "wire transmission" as any communication "made in whole or part" through wire facilities. The Senate Report explains the need for this qualification by noting that "most telephonic and telegraphic communications are transmitted at least in part by microwave transmission" and that FISA is only intended to apply to "those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted" within the United States or where the interception "targets" a U.S. person or intentionally intercepts a radio transmission in which the sender and all of the intended recipients are in the United States (i.e., purely domestic microwave communications). S. REP. NO. 95-604 at 33. Thus, FISA was crafted with some intentional definitional complexity specifically to exclude non-targeted interception of international communications, including those with one end in the United States.

[6] Attorney General Levi testified:

Unfortunately, these outdated technical distinctions are now inadequate to address certain technology developments that have occurred since the enactment of FISA, including the transition from circuit-based communications to packet-based communications; the globalization of communications infrastructure; and the development of automated monitoring techniques, including data mining and traffic analysis.

Because of these technology developments, much legitimate foreign signals intelligence activity directed at finding signals of interest (that is, activity not directed at targeted individuals in the United States but rather at finding information with foreign intelligence value for counterterrorism or counter-proliferation purposes from monitoring legitimate foreign intelligence channels or targets, including their international communications to and from the United States) can no longer be conducted within the framework envisioned by FISA. Activities previously accomplished by radio interceptions or conducted abroad (and intentionally excluded from FISA procedures) are increasingly only possible through interceptions conducted at communication switches within the United States (including "transit intercepts" of wholly foreign communications) or at switches or fiber optic cable repeaters that carry significant U.S. person or domestic traffic as well (resulting in the "substantial likelihood" of collateral intercepts), thus, potentially triggering FISA and its procedural requirements in circumstances that were not contemplated at enactment.

A detailed discussion of these technology developments—including how they interact with FISA and how FISA procedures are being triggered in circumstances such as transit intercepts, collateral intercepts, and through automated signals intelligence processing activities that FISA was never intended to cover (and for which current FISA warrant procedures are ill-suited)—is included in my recent article, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, published in the Yale Journal of Law and Technology, a copy of which is attached and incorporated herein by reference. [7]

Preemption, not technology, poses the more difficult policy problem.

The fundamental challenge to existing law and policy, however, is not technological—if it were, resolution might be more easily accomplished. The real challenge arises from the need to pursue preemptive strategies against certain potentially catastrophic threats from

---

> But, as I have pointed out, the bill is by its definition limited to the interception within the United States by electronic surveillance, as defined, of foreign intelligence information. The bill does not purport to cover the interceptions, other than by the use within the United States of devices such as wiretaps or microphones, of international communications.

Levi, *supra* note 3, at 12-13. And, *see* note 5 *supra*.

[7] K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128 *(Spring 2007) available at* http://ssrn.com/abstract=959927.

transnational terrorism and nuclear weapons proliferation that in part necessitate using electronic surveillance methods that were not originally intended to be covered by FISA or related warrant procedures (and that don't easily lend themselves to such practices) but that increasingly affect the privacy and civil liberties interests of persons in the United States. [8]

The challenge is in crafting a new framework—one that is both enabling of legitimate foreign intelligence activities and yet protective of privacy and civil liberties—to govern the use of signals intelligence methods (particularly, those methods that were originally not intended to be subject to FISA and for which the existing FISA procedures are not well-suited) against new national security threats when these uses increasingly impact the same privacy and civil liberties interests that FISA *was* originally intended to address.

The policy conundrum is in reconciling the rigid law enforcement-derived policies and procedures intended to govern the use of electronic surveillance technologies to monitor the activities of known subjects with the more amorphous foreign intelligence and national security strategies needed to identify previously unknown threats (in order to develop the kind of actionable intelligence necessary for preemption). These activities were previously subject to disparate and often conflicting policy regimes—the former subject to formal judicial warrant procedures under FISA and the latter at the sole discretion of the executive with little oversight or review.

The administration's proposals: exclude signals intelligence from FISA

The proposed Foreign Intelligence Surveillance Modernization Act of 2007 ("FISMA") would amend FISA to exclude most foreign and international signals intelligence activity from triggering FISA warrant requirements by simplifying the definition of "electronic surveillance" for purposes of the statute to interceptions (1) intentionally targeting a particular, known person reasonably believed to be in the United States, or (2) intentionally acquiring the contents of communications when all parties are reasonably believed to be in the United States. The effect of these changes would be to exclude any non-targeted interception of international communications from FISA or its warrant requirements even if one party to the communication was in the United States. [9]

Although it can be argued persuasively that such a proposal merely updates—in a way no longer dependent on outdated technical distinctions—the original legislative intention for FISA to not cover these kinds of activities, in our view it fails to acknowledge the political reality that certain of these "foreign" activities increasingly infringe on the

[8] It is beyond the scope of these comments to delineate precisely where the line should be drawn between threats to national security that require a preemptive approach and those that remain amenable to traditional reactive law enforcement methods. However, it is axiomatic that national security assets, including foreign intelligence surveillance capabilities, should be employed only against true threats to national security and not for general law enforcement or social control purposes.

[9] As discussed below, another effect of this definitional change would be to exclude from FISA non-targeted collection of non-content or "transactional" information about communications.

legitimate privacy expectations of persons in the U.S. in ways and degrees not previously contemplated and, therefore, as a *policy* matter, certain of these activities with the potential for significant domestic impact may now require some form of explicit statutory authorization and oversight mechanism external to the executive branch to create political consensus, reassure the public, and provide democratic accountability. [10]

Thus, regardless of whether the executive indeed has inherent authority to conduct foreign intelligence surveillance activities—including those that intercept international communications to and from the United States—without such explicit statutory authority or oversight, our system of government works best, and public confidence is best maintained, only when the branches of government work together in consensus and the broad parameters of procedural due process protections are publicly debated and agreed.[11]

In discussing the intentional exclusion of NSA signals intelligence activities from FISA, the 1977 Senate Report No. 95-604 at 64 states:

> The activities of the NSA pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the NSA and the surveillance of Americans abroad raises problems best left to separate legislation.

Because of the difficulties in continuing to maintain separate policy regimes, particularly for foreign intelligence activities outside of FISA that may substantially affect the privacy and civil liberties interests of large numbers of persons in the U.S. in ways not previously contemplated,[12] it may be time to address these conceptual and technical difficulties

---

[10] It should be noted that FISA itself was "not a response to some presumed constitutional requirement of a judicial warrant as a condition of the legality of surveillance undertaken for foreign intelligence purposes. Such a requirement has not been the holding of the courts …" rather, FISA was enacted to bring consistency to fragmented legislation, judicial decisions, and administrative action and practice in these areas. FISA was a political compromise in which the inherent but undefined executive power to conduct foreign intelligence surveillance explicitly acknowledged by the courts was "augmented" by legislation in return for subjecting domestic foreign intelligence surveillance to a statutory regime, including statutory warrant procedures. *See* Levi, *supra* note 3, at 8-9, 16.

[11] I take no position in these comments on the important constitutional issue of whether the executive has sole, primary, or shared authority to conduct foreign intelligence activities pursuant to his commander-in-chief or foreign affairs powers. My suggestion for seeking legislative authority for programmatic approval of certain foreign intelligence activities with a substantial impact on U.S. persons, as is implicit in these comments, is based on my view that it is advisable for policy reason to put such activity on an explicit statutory foundation in order to engender the broadest possible political, judicial, and public support for legitimate and necessary foreign intelligence activities vital to the national security of the United States.

[12] It should be noted that NSA foreign signals intelligence activities were likely to affect many fewer persons in the U.S. thirty years ago when FISA was enacted than in today's globalized economy and communications networks—both because more people in the U.S. are now likely to be engaged in international communications but also because it is increasingly difficult to actually differentiate foreign,

directly rather than to ignore them by simply excluding all such activity from any legislative reach. [13]

Requiring traditional FISA warrants for signals intelligence is unworkable.

Many critics of the administration's proposed amendments concede that changes in technology have undermined the existing FISA framework. [14] However, they argue that rather than excluding non-targeted or foreign intelligence activities from FISA as proposed by the administration, that these technology developments justify extending existing FISA warrant requirements to all electronic surveillance activities in which U.S. person or domestic communications are likely to be intercepted, even if no U.S. person or communication is targeted and the communication is merely acquired incidental to the targeting of legitimate foreign intelligence targets. But, in doing so they ignore the fundamentally different requirements and circumstances of non-targeted or foreign signals intelligence and targeted domestic wiretaps. [15]

If the existing FISA warrant procedures were to be strictly applied to all foreign intelligence activities then no useful signals intelligence activity of any kind would be possible—there would simply be no procedure under which electronic signals intelligence could be employed to uncover unknown connections or threats from persons in the United States communicating or conspiring with known al Qa'ida or affiliated operatives. Such an outcome would, of course, have significant national security ramifications.

In any case, there is no constitutional requirement for warrants in these circumstances.[16] For a discussion of the relevant constitutional constrains, see *Hearing on Modernizing the*

---

international, and domestic communications within a globalized packet-based communication network in which traffic is routed dynamically and where local addressing information can be used globally. See *The Ear of Dionysus*, *supra* note 7, at 143-145, 146-147, 146 n.50, and 147 n.51.

[13] We are not advocating that all foreign intelligence surveillance activity come under a statutory scheme—indeed, there would be significant separation of powers issues involved if it did—but only that a mechanism to approve specific programs or kinds of signal intelligence activity where there is a substantial likelihood of acquiring the contents of U.S. persons be considered for policy reasons in order to garner the widest possible political, judicial, and public support for legitimate foreign intelligence activities.

[14] *See, e.g.*, Center for Democracy & Technology, *Modernization of the Foreign Intelligence Surveillance Act (FISA): Administration Proposes Broad Warrantless Surveillance of Citizens* (April 18, 2007).

[15] Foreign signals intelligence activities have many legitimate and necessary purposes beyond counterterrorism and counter-proliferation that need to be considered when crafting any framework that might inadvertently curtail these vital activities. It is beyond the scope of these comments, and, in any case, would be inappropriate in open session or public remarks, to discuss these additional requirements.

[16] Indeed, absent the FISA statute, there is no general warrant requirement for foreign intelligence surveillance under the Fourth Amendment. *See, e.g.,* United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980) (acknowledging the foreign intelligence exception to the Fourth Amendment warrant requirement), cert. denied, 454 U.S. 1144 (1982); *see also* United States v. United States District Court [Keith], 407 U.S.

Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence, 109th Congress, at 7-10 (Jul. 19, 2006) (Testimony of Kim Taipale, Center for Advanced Studies in Science and Technology Policy). [17]

Further, it is not clear in any case what substantive protections warrant procedures would add in this context—either they would prevent any signals intelligence activity from being used preemptively to identify threats (with devastating effect on the ability to gather foreign intelligence for any purpose), or they would become pro forma ministerial procedures with no substantive protections for privacy or civil liberties.

That the conventional law enforcement-derived warrant procedures might be an inappropriate method for authorizing legitimate foreign intelligence activities or might be ineffective to protect civil liberties when applied to certain kinds of intelligence activities is not a novel proposition. Testifying before the Church Committee in 1975, then-Attorney General Edward Levi suggested that FISA should explicitly include provisions for the approval of "programs of surveillance" in foreign intelligence situations where "by [their] nature [they do] not have specifically predetermined targets" and where "the efficiency of a warrant requirement would [therefore] be minimal." [18]

Programmatic approvals for certain foreign signals intelligence.

As noted above, the administration's proposals would exclude all non-targeted or non-domestic surveillance activity from FISA jurisdiction. While such an outcome would be in keeping with the intent of FISA as enacted, for the reasons discussed above, we think it would be useful for both Congress and the administration to consider whether a statutory mechanism for programmatic approval of certain foreign signals intelligence activity where there is a substantial likelihood of acquiring U.S. persons international or domestic communications would be appropriate. Such a mechanism would provide additional

---

297, 321-22 (1972) (warrant required for domestic security electronic surveillance, but Court explicitly disclaims any intent to decide whether warrant clause even applies to surveillance of foreign powers or their agents.). Further, there is no Fourth Amendment requirement for a warrant for incidental collection to a lawful intercept. Even under the stricter provisions governing ordinary criminal electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. §§ 2510-2521, incidental interception of a non-targeted person's conversations during an otherwise lawful surveillance would not be a violation of the Fourth Amendment. *See* United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985); *and* United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973).

[17] Available at http://intelligence.house.gov/Reports.aspx?Section=141. *See also The Ear of Dionysus*, *supra* note 7, at 134 n.16, 147 n.53, and158 n. 89.

[18] Likewise, even while requiring some form of judicial approval for *domestic* security surveillance, the court in Keith, *supra* note 16, suggested that different standards would be reasonable under the Fourth Amendment for security cases, noting that in such surveillance "the emphasis of … intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency" and thus "the focus of … surveillance may be less precise than that directed against more conventional types of crime" and that "exact targets of such surveillance may be more difficult to identify."

political, judicial, and public assurance that any foreign signals intelligence activity with a significant impact on domestic privacy or civil liberties was being lawfully conducted.

Programmatic approvals.

We have previously advocated that an explicit statutory mechanism be enacted, incorporating democratic checks-and-balances, for programmatic approval of certain foreign intelligence activities where there is a substantial likelihood of intercepting U.S. communications; in particularly, for those activities targeting specific foreign channels or targets, or using automated analysis or monitoring of foreign communication channels, where there is the likelihood of significant collateral intercepts of U.S. communications.

Various institutional mechanisms for programmatic approval and oversight of foreign intelligence surveillance programs have been suggested in connection with the NSA Terrorist Surveillance Program. These proposals have included executive, legislative, and judicial bodies. [19] Although I have briefly discussed the pros-and-cons of legislative versus judicial approvals on pages 10-12 of my HPSCI testimony, [20] I have not previously advocated any specific approval mechanism or standards. More recently, I have personally become persuaded by the arguments of John Schmidt, a former senior Justice Department official, that a statutory legal structure enacted by Congress authorizing direct judicial involvement in programmatic approvals would be most appropriate in order to foster the requisite political and public confidence in the legality of any authorized surveillance activities. [21]

The problem with the FISA procedures as currently constituted is that FISA provides only a single binary *a priori* threshold for authorizing any electronic interception—probable cause that the target is an agent of a foreign power. Unfortunately, even extensive contact with a known terrorist may not be procedurally sufficient to satisfy the current statutory requirements for a FISA warrant, and, more importantly, such contacts

---

[19] Compare, for example, Judge Richard Posner's proposal for an executive branch steering committee for national security electronic surveillance (*Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence*, 109th Congress (Jul. 19, 2006) (Testimony of Judge Richard A. Posner) at 4-5); the proposed Terrorist Surveillance Act of 2006, S.3931, 109th Congress (2006) (the DeWine bill) (oversight by special Congressional committees); the proposed National Security Surveillance Act of 2006, S.3876, 109th Congress (2006) (the Specter bill) (FISA court approval and oversight); John Schmidt, *Together Against Terror*, LEGALTIMES (Jan. 15, 2007) (FISC); and, the Electronic Surveillance Modernization Act, H.R. 5825, 109th Congress (2006) (the Wilson bill) (passed by the House on Sep. 28, 2006 and referred to the Senate Committee on the Judiciary) (requiring Congressional oversight but allow submission to the FISC for review).

[20] *See* note 17 *supra*.

[21] *See* John Schmidt, *Together Against Terror*, LEGALTIMES (Jan. 15, 2007); *The Ear of Dionysus*, *supra* note 7, at 156 n.84. Additional reporting and disclosure requirements, as well as enhanced oversight and review procedures should be considered as well.

may only be discoverable through non-targeted or foreign directed signals intelligence activities in the first place. [22]

The FISC Orders of January 10, 2007.

Details of the FISC orders issued January 10, 2007 (authorizing certain activities previously carried out pursuant to Presidential authority under the NSA Terrorist Surveillance Program) [23] have not been publicly disclosed and the Justice Department has indicated that it is not prepared to release the orders to the public. [24] Speculation about the nature of the FISC orders has included discussion of whether they take the form of "anticipatory warrants" that would authorize surveillance in the future if certain factual predicates were to occur (including, for example, a known terrorist communicating with a someone in the U.S.). [25]

The Department of Justice has specifically denied, however, that these orders are "programmatic" in nature thus it is unlikely that they provide sufficient solution to the entirety of the problem of reconciling foreign signals intelligence activities with targeted domestic surveillance as discussed in these comments. Therefore, we still advocate a specific statutory basis for broader FISC jurisdiction and specific authority for "programmatic" approvals. Nevertheless, at the very least, it seems appropriate that an explicit statutory basis to support the January 10, 2007 FISC orders should be enacted.

Attorney General Levi foreshadowed an outcome in which anticipatory or programmatic warrants might be the appropriate mechanism to manage certain foreign signals intelligence activities when he suggested in his testimony to the Church Committee that a different kind of warrant based on submitting programs of surveillance (designed to gather foreign intelligence information essential to the security of the nation but not based on individualized suspicion) for judicial review might be developed. Here he cited Justice Powell's opinion in Almeida-Sanchez v. United States, 413 U.S. 266 (1973), in which the possibility of using "area warrants" to obtain "advance judicial approval of the decision to conduct roving searches on a particular road or roads for a reasonable period of time" was suggested approvingly. Levi went on to suggest that the development of any such new kind of extended warrant would benefit from an explicit statutory basis.

---

[22] For example, unlike with previous threats from other nation states or from ordinary crime, there may be no independent way to establish a connection to a foreign terrorist or proliferation group without the use of signals intelligence, particularly in cases where the recruitment and all contacts is conducted solely by electronic communications, for example, over the Internet.

[23] Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman, and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 2007), *available at* http://fas.org/irp///agency/doj/fisa/ag011707.pdf.

[24] *See* Government's Supplemental Submission Discussing the Implications of the Intervening FISA Court Orders of Jan. 10, 2007 at 8-15, *ACLU v. NSA* (No. 06-CV-10204) (submission filed Jan. 24, 2007).

[25] The use of anticipatory warrants was upheld in U.S. v. Grubbs, 126 S. Ct. 1494, 1500 (2006) (warrant containing "triggering conditions" is constitutional).

He also suggested, however, that in dealing with foreign intelligence surveillance "it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections." Thus, programmatic approvals through statutory administrative or congressional authority should also be considered.

Non-content transactional data.

Although FISA currently has provisions for authorizing the targeted collection of non-content information—the FISA pen register and trap-and-trace provisions—it does not provide any procedures for authorizing even specific but non-targeted traffic or link analysis that may be required—and wholly reasonable—in the context of foreign signals intelligence to identify certain connections or threats.

For example, known patterns of terrorist communications can be identified and used to uncover other unknown but indirectly related terrorists or terrorist activity. Thus, for instance, in the immediate aftermath of 9/11 the FBI determined that the leaders of the 19 hijackers had made 206 international telephone calls to specific locations in Saudi Arabia, Syria, and Germany. It is believed that in order to determine whether any other unknown persons—so-called sleeper cells—in the United States might have been in communication with the same pattern of foreign correspondents the NSA analyzed Call Data Records (CDRs) of international and domestic phone calls obtained from the major U.S. telecommunication companies.

Undertaking such an analysis seems reasonable, particularly in the circumstances immediately following 9/11, yet FISA and existing procedures do not provide *any* approval or review mechanism for determining such reasonableness or for authorizing or governing such activity because FISA simply did not contemplate the current need for approval of specific—but non-targeted—pattern-based data searches or surveillance. [26]

Further, while it is well settled law that dialing or signaling information is entitled to lesser constitutional protection from disclosure than is content, [27] FISA as currently enacted is somewhat confusingly inconsistent about how such information is to be treated even in cases of targeted acquisition. FISA currently defines "content" to include "the identity of the parties to such communication or the existence" of the communication (*i.e.,* transactional information) but it also authorizes orders for pen registers and trap-and-trace devices to collect such information under a lesser standard than the statute requires for "content" intercepts.

---

[26] It is important to point out that the kind of automated traffic or link analysis being discussed here is not the undirected "data mining" to look for general indicia of "suspicious behavior" that rightly has civil libertarians concerned about fishing expeditions or general searches to examine all communication flows in the manner of a general warrant. See *The Ear of Dionysus, supra* note 7, at 150-156, 154 n.77. For a detailed discussion of general issues related to data mining, see the references in note 70, *id*. at 152.

[27] Smith v. Maryland, 442 U.S. 735 (1979).

The administration's FISA modernization proposals would address both the failure to anticipate the need for non-targeted traffic analysis and the inconsistency in statutory language for targeted collection by changing the definition of content to exclude transaction data and by simplifying the definition of "electronic surveillance" to only cover content interception. [28]

Again, while there is a strong case that the administration proposal is consistent with existing law and the original intent of FISA, nevertheless—for the same reasons set forth above regarding programmatic approval of content based signals intelligence—some statutory procedure to authorize and approve directed traffic or link analysis of transactional communication records where there is a significant impact on U.S. persons or domestic communications seems desirable as a matter of public policy.

The same kind of approval mechanisms discussed above for programmatic approvals might be applicable in these circumstances as well, recognizing, of course, that approvals for these activities should be subject to a lesser standard than those involving content, consistent with existing law.

Conclusion: FISA must be updated.

FISA as currently enacted fails to adequately enable legitimate and necessary foreign intelligence surveillance activity or to adequately protect privacy and civil liberties.

The administration is seeking to explicitly exclude from FISA statutory requirements those non-targeted or foreign signals intelligence activities that were not originally intended to be included in the FISA regime and that don't fit easily within its existing framework. Although we agree that this proposal is wholly consistent with the original intent of FISA, we are concerned that these kinds of activities increasingly impact the same domestic privacy and civil liberties interests that the political compromise leading to FISA was intended to address.

On the other hand, the critics of the administration's proposals are arguing simply to extend ill-suited FISA warrant procedures over activities that have different requirements and considerations than those for which FISA was designed and enacted. Force fitting these existing procedures to cover all signals intelligence activities that may affect U.S. persons is simply unworkable, is not constitutionally required, and would severely frustrate the ability to gather foreign intelligence information vital to the national security and interests of the United States.

The Center for Advanced Studies urges Congress to consider an adaptive legislative framework that will enable legitimate foreign intelligence activities while still protecting privacy and civil liberties; and that explicitly recognizes the different requirements and circumstances of signals intelligence and targeted wiretaps.

---

[28] Targeted collection of transactional information would still be subject to the pen register and trap-and-trace provisions of FISA,

We urge Congress to consider enacting an institutional mechanism for the programmatic approval, oversight, and review of legitimate foreign signals intelligence activity or programs where such activity is likely to have substantial impact on domestic privacy or civil liberties interests, as well as to provide some explicit guidelines governing how information derived from such programs can be reasonably used to protect the national security of the United States while still protecting privacy and civil liberties consistent with existing laws.

FISA as currently constituted is viable only for monitoring the activities of known agents of a foreign power but it is wholly ineffective for enabling or constraining the use of foreign signals intelligence to help identify threats in the first place or otherwise gather signals with foreign intelligence value to the United States. FISA must be updated to address these failures in order to protect both national security and individual freedom. Both values are indispensable and must be reconciled.

May 1, 2007.