Testimony of

James X. Dempsey

September 25, 2007

Statement of James X. Dempsey
Policy Director
Center for Democracy & Technology*

before the
Senate Committee on the Judiciary

Strengthening FISA: Does the Protect America Act
Protect Americans' Civil Liberties and Enhance Security?

September 25, 2007

Chairman Leahy, Ranking Member Sen. Specter, and Members of the Committee, thank you for the opportunity to testify this morning.

The Director of National Intelligence has laid out three basic requirements for FISA legislation:

? No particularized orders for surveillance designed to intercept the communications of foreigners overseas, but a means to compel service provider cooperation when those communications are accessible inside the US.
? A court order for surveillance of Americans.
? Immunity for service providers that cooperate with the government.

All three of these goals can be achieved in a way that serves both the national security and civil liberties, guided by the principles of operational agility, privacy and accountability. The Protect America Act, adopted last month under intense pressure, fails to achieve the Administration's stated requirements in a rational and balanced way. We will outline here how to achieve the Administration's goals within a reasonable system of checks and balances, suited both to changes in technology and the national security threats facing our nation.

I. No Particularized Orders for Surveillance Designed to Intercept the Communications of Foreigners Overseas

A. The Debate Concerns Communications To and From People in the US

The debate over FISA this year has not been about terrorism suspects overseas talking to other people overseas. For a long time, there has been agreement among Members of Congress in both parties, and even in the civil liberties community, that a court order should not be required for interception of foreign-to-foreign communications even if the surveillance occurs on US soil. To achieve balanced resolution of this sometimes heated debate, we should put aside any generalized rhetoric about surveillance of terrorists abroad. That is not the issue.

Instead, the debate for the past year has been over the rights of American citizens and others inside the US, where the Constitution's protections apply even to national security activities. The NSA argues that it is only "targeting" foreigners overseas, but it is certain that that some of those persons overseas will communicate with people in the US. When the government intercepts communications of citizens and others inside the US, it is interfering with the privacy of those persons inside the US, even if the government is "targeting" persons overseas.

The NSA argues, with justification, that its needs agility and speed when targeting persons overseas and should not need to prepare applications for particularized orders for foreign targets overseas when the interception of those communications may not interfere with the rights of anyone in the US. It seems likely that a certain percentage of foreign intelligence targets overseas will communicate only with other foreigners overseas, so it seems reasonable to assume that a certain percentage (perhaps a very large percentage) of surveillance targeted at persons overseas will not affect the rights of people in the US. Furthermore, the NSA in most cases when it is targeting a person overseas cannot be sure in advance whether the particular targeted person overseas will sometime in the future have a communication with someone in the US. Therefore, it is reasonable to allow NSA to begin surveillance of targets overseas without a particularized order on the presumption that surveillance targeted at a person overseas will not interfere with the rights of Americans.

However, it is also certain that some of those persons of interest to NSA overseas will communicate with people in the US. Some percentage - most likely a growing percentage - of NSA's activities targeted at persons overseas result in the acquisition of communications to and from the US. The individuals in the US retain their reasonable expectation of privacy in their communications even when they are communicating with persons overseas. When the government "listens" to both ends of the communication - as it admits it will do in some cases - it infringes on the privacy rights of the Americans.

When surveillance will intrude on the privacy of persons inside the United States, the question of how to conduct that surveillance - what facilities (places) to search and what communications (things) to seize -- is one our Constitution generally commits to prior judicial review. It should be a judge who decides in the first place that the government's activities are reasonably designed to intercept the communications of terrorists or other foreigners overseas likely to contain foreign intelligence and are not likely to unnecessarily intercept the communications of innocent Americans.

The Analogy to Wiretaps in Criminal Investigations Shows That a Warrant Is Crucial

Law and practice governing more familiar wiretaps in criminal cases may help explain the situation here: If the government is wiretapping the phone of a Mafia don, it will inevitably intercept communications with a range of other persons, from the don's criminal associates to the pediatrician for his children. The government will listen to the communications with the pediatrician to determine who he is and whether he is involved in the don's criminal conduct. If the police overhear the pediatrician discussing insurance fraud with the don, they can use that evidence against the doctor, even if they did not suspect at the outset of the surveillance that he was involved in criminal conduct. On the other hand, the doctor may be innocent, but the police may initially suspect he is in league with the don, and may share that information with the FBI, who may instigate a fruitless but damaging investigation of the doctor before they conclude he is innocent.

In this case, if the surveillance is court authorized, the doctor has no ground to complain about the monitoring of his calls, whether he is guilty or innocent. As has been noted, "a valid eavesdropping order of necessity permits the interception of communications of at least two parties." People v. Gnozzo, 31 N.Y.2d 134, 335 N.Y.S.2d 257, 265, 286 N.E.2d 706, 711 (1972). On the other hand, if the surveillance is not court authorized, the doctor has both constitutional and statutory grounds to complain. The fact that the government was targeting the don does not diminish the injury to the doctor - he has a claim for Fourth Amendment violation of his rights, and he has a civil claim under Title III for warrantless surveillance.

As in the criminal case, the presence or absence of a court order makes all the difference to the rights of the non-targeted person.

B. Searches Without a Warrant Are Presumptively Unconstitutional

All searches, even national security searches, are subject to the Fourth Amendment. They must meet the reasonableness standard. In order to be reasonable, searches must be based on particularized suspicion, they must be limited in scope and duration and, with rare exceptions, they must be conducted pursuant to a warrant.

Several courts have held that a warrant is not required for particularized searches to collect foreign intelligence where there is reason to believe that the subject of the search is an agent of a foreign power engaged in espionage or

terrorism. The Supreme Court has never ruled on the issue and it must be considered unresolved. However, no court has ever permitted warrantless searches as broad and standardless as those authorized under the PAA. For example, while US v Butenko, 494 F.2d 593 (3rd Cir. 1974), held that a warrant is not required for foreign intelligence surveillance, it went on to emphasize that, even in national security cases, "The foundation of any determination of reasonableness, the crucial test of legality under the Fourth Amendment, is the probable cause standard." 494 F.2d at 606. Likewise, in US v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980), the Fourth Circuit held that "the government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborators."

The PAA falls far short of the standards enunciated in Butenko and Truong. It is not limited to searches of the communications of foreign powers or agents of foreign powers. Searches under the PAA are not based on probable cause. They are not reasonably limited in duration.

Given the utter lack of standards, it is highly likely that a search under the PAA of the international communications of US persons would be unconstitutional. If a search is conducted without a warrant, "[t]he scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." Terry v. Ohio, 392 U.S. 1, 17 (1968). The PAA does not set forth any limits tied to any special circumstances, other than the generalized need to collect any foreign intelligence.

C. The PAA Provides Inadequate Judicial Review of Surveillance Activities Likely to Affect the Rights of Americans

DNI McConnell has accepted the principle of judicial review and the PAA has a procedure for FISA court review of certain procedures, but it is woefully inadequate. The minimal judicial review in the PAA does not protect the rights of Americans and does not provide assurance of the Act's constitutionality:

? The PAA does not submit the right questions to judicial review. The PAA requires the Administration to submit to the FISA court procedures either for ensuring that the persons being targeted are outside the U.S. or for determining that the acquisitions conducted under 105B do not constitute electronic surveillance. We have no doubt that the government will easily meet either or both requirements. The additional, and much more important, question that should be reviewed is whether, in choosing among all the foreigners overseas, NSA uses procedures reasonably designed to identify and collect the communications of those persons or entities whose communications have foreign intelligence value. This would seem to be the minimum standard for national security surveillance. Such a limitation may be imposed on the NSA by Section 105B or E.O. 12333, but given the Fourth Amendment implications of electronic surveillance, it should be judicially enforced.
? The PAA sets a standard of review - "clearly erroneous" - that is too low. The clearly erroneous standard is used by appellate courts to review trial court findings of fact, and it is appropriate for the Executive Branch's determination under FISA that information is foreign intelligence. It is entirely unsuited to ex parte review of the threshold search and seizure standards involving the protection of Fourth Amendment rights.
? The review provided in the PAA comes too late - after the surveillance has begun. That may have been considered necessary when the Administration claimed that there was a crisis and that surveillance needed to start immediately in order to prevent an attack during August. Now that the government is operating under the PAA, it has time to define and refine its targeting and filtering criteria so that they can be submitted to the FISA court for prior judicial review.
? The review under the PAA does not result in a court order authorizing surveillance and compelling corporate cooperation.

After-the-fact minimization of seized communications cannot take the place of judicial review of the decision of where to search in the first place. Because the minimization rules undoubtedly (and justifiably) will allow the retention and use of some communications of Americans captured under a program "targeting" foreigners overseas, some independent (although not necessarily particularized) review of targeting practices is necessary upfront.

D. A More Effective and Balanced Approach: Blanket Orders to Target Persons Abroad

In short, it is unreasonable in a practical sense to require particularized orders when targeting persons overseas, but it is unreasonable in a constitutional sense to leave solely to unguided Executive Branch discretion surveillance activity in the US that will undeniably result in the interception of communications to and from Americans.

It is possible to balance the Administration's argument that a particularized court order is not feasible for interception activities targeted at persons overseas against the need to ensure that the government's activities do not unnecessarily or broadly infringe on the communications privacy of persons inside the US.

At the very least, the FISA court should review whether the government's selection and filtering methods are reasonably likely to ensure that (1) the communications to be intercepted are to or from non-US persons overseas and (2) such communications contain foreign intelligence. The second prong of this standard affords the government wider latitude than the "agent of a foreign power" standard. It should be made clear that the court cannot review the specific selectors (for example, specific phone numbers) or filters, but rather reviews the criteria for determining those selectors and filters.

A court order authorizing a program of surveillance directed at persons overseas has three major advantages:

? It creates jurisdiction in the FISA court for oversight of the implementation of the program, the application of the minimization rules, and the process for seeking an order when the surveillance begins to infringe significantly on the rights of people in the US.
? It provides the communications companies the certainty they deserve if they are expected to cooperate with wiretapping. Reliance on Attorney General certifications may leave corporations unsure of their liability.
? It is more likely to be constitutional. The PAA authorizes a program of warrantless surveillance far broader than anything approved by any court. It is very risky for the government to be proceeding with a program of national security significance whose constitutionality is highly debated. The purpose of FISA was to place national security surveillance on a firm constitutional footing. If the NSA's surveillance does disclose a terrorist threat inside the US, the government should have the strongest constitutional basis for using information acquired under the program to carry out arrests or further domestic surveillance.

II. A Court Order for Surveillance of Americans

A. "Targeting" Is Not the Standard for Assessing Fourth Amendment Rights

The Administration agrees that the surveillance of Americans should be subject to a regular order under FISA. But the Administration argues that a court order is needed only when it is "targeting" a US person in the US, and that it should be able to intercept the communications of American citizens and other US persons so long as it is not "targeting" the US person. For constitutional purposes, "targeting" is not the relevant question. Indeed, in 1978 (after FISA was enacted), the Supreme Court rejected the concept of "targeting" as the basis for evaluating Fourth Amendment rights. Rakas v. Illinois, 439 U.S. 128 (1978). Instead, Fourth Amendment rights turn on whether a person has a reasonable expectation of privacy and whether that expectation was infringed upon. Persons in the US clearly have a reasonable expectation of privacy in their communications, and the government infringes on that right when it intercepts those communications. Katz v. United States, 389 U.S. 347 (1967) and Berger v. New York, 388 U.S. 41 (1967).

It makes no difference to the rights of Americans that the people overseas they are communicating with have no Fourth Amendment right. In a recent case, the Supreme Court held that when two people share a space and one of those persons waives her Fourth Amendment rights, the second person does not lose his. A search taken over the objection of the second party, the Supreme Court held, is unconstitutional even though the other party no longer had a Fourth Amendment right. Georgia v. Randolph, 547 U.S. ___ (2006).

B. Minimization Is Not Sufficient to Protect the Rights of Americans

The Administration's one word answer to concerns about the effect of the PAA on the rights of Americans is "minimization." CDT has prepared and will submit for the record a lengthy analysis on "minimization." Our analysis shows that reliance on "minimization" to defend the PAA fails for two reasons:

(1) Even if "minimization" meant that the government discarded all intercepted communications of Americans, it would not cure the damage done to privacy when the communications are intercepted in the first place. The police cannot come into your house without a warrant, look around, copy your files and then claim no constitutional violation because they threw everything away after they looked at it back at the station house.

(2) Under FISA, "minimization" does not mean that the government must discard all of the communications of people in the US "incidentally" collected when the government is targeting someone overseas. To the contrary, the "minimization" that would be applicable to the PAA permits the government to retain, analyze, and disseminate to other agencies the communications of US citizens.

Under the "minimization" rules applicable to the PAA, the American citizen talking to relatives in Lebanon, the charities coordinator planning an assistance program for rural areas of Pakistan, the businessman buying or selling products in the Middle East, or the journalist gathering information about the opium trade in Afghanistan- all while sitting in the US - might have their international calls or emails monitored, recorded and disseminated without judicial approval or oversight if the NSA or another agency, in its sole discretion, decided to "target" the persons they were talking to overseas.

One of the seminal wiretap cases, Katz v. US, 389 U.S. 347 (1967), made it clear that minimization does not make a warrantless search constitutional. In Katz, the government agents had probable cause. They limited their surveillance in scope and duration to the specific purpose of collecting the target's unlawful communications. They took great care to overhear only the conversations of the target himself. On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them. None of this saved the surveillance constitutionally. The Supreme Court said:

It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," Agnello v. United States, 269 U.S. 20, 33, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . ." Wong Sun v. United States, 371 U.S. 471, 481 -482. "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," United States v. Jeffers, 342 U.S. 48, 51 ... . [389 U.S. at 356 - 357]

It is apparent that the concept of minimization as applied by the NSA in recent years has permitted the retention and dissemination of considerable quantities of information about US persons. Newsweek reported in May 2006 that between January 2004 and May 2006, NSA had supplied the names of some 10,000 American citizens to various interested officials in other agencies. It has also been reported that, after 9/11, the head of the NSA changed internal interpretations of the redaction procedures to allow routine dissemination of identifying information about US persons, presumably on the ground that information identifying U.S. persons was necessary for the FBI and other agencies to follow-up on the intelligence. According to one report, under the NSA's new practice, the FBI was flooded with information identifying U.S. persons.

The terrorist watch list is a perfect example of how the wider dissemination of information can affect ordinary Americans. The watch list now contains over 700,000 entries, created on the basis of reports from a range of intelligence agencies. The list is growing at the rate of 20,000 entries a month. A recent study by the Department of Justice Inspector General found that, even after vetting by the Terrorist Screening Center, 38% of the records on the list contained errors or inconsistencies. In 20% of the cases that have been resolved where members of the public complained that they were inappropriately lists, the complaint was resolved by entirely removing the name from the watchlist. The list, however, is secret. Individuals must guess as to whether they are on it in order to seek redress. The list is used not only as the basis for the passenger screening program that affects 1.8 million air travelers a day. The watchlist feeds into the Violent Gang and Terrorist Organization File, which is made available through the NCIC

to over 60,000 state and local criminal justice agencies and may be relied upon by police in ordinary encounters with citizens on a daily basis.

The intelligence agencies are under Congressional and Presidential mandates to share information, including information about US persons. They are doing so, and they are relying on shared information, including erroneous information, to make decisions affecting people in their ordinary lives. Minimization is no longer being applied - and probably should not be applied - to block dissemination of information about US persons. There need to be other protections.

C. A More Effective and Balanced Approach

There needs to be a mechanism for addressing those situations where the communications of an American are intercepted as a result of activities designed to intercept the communications of persons reasonably believed to be overseas. Minimization can help address this problem, but, as Katz held, minimization without a court order does not make a search constitutional.

Minimization may be sufficient to address the truly incidental collection of the communications of persons inside the US. However, when the surveillance of the communications of an American becomes significant, particularized court review should be triggered.

The development of a standard for particularized review should take into account the fact that the NSA generally does not analyze communications in real time and does not analyze all of the communications it intercepts. The best approach may be through the use of periodic reports to the FISA court under the program warrant we recommended in section I. Such periodic reports about the results of blanket searches targeted at the communications of persons overseas would allow the court to identify when certain surveillance activity is significantly infringing on the rights of Americans.

The Administration complains that a "significant number" standard is unworkable, arguing that it often is not possible to tell whether a communication is with a US person. We believe that these questions can be resolved by the court, applying the Fourth Amendment and using the Administration's own processes for determining whether a communication involves a US person. Administration officials have assured the Congress that they are able to distinguish US person communications for purposes of applying the minimization rules. While those minimization procedures no longer block dissemination of US person information, they do require an assessment be made as to whether information is about a US person. This same determination can be used as the basis for periodic reports to the FISA court. And the court can determine whether surveillance is affecting the Fourth Amendment rights of Americans.

III. Communications Companies Deserve Immunity for Cooperation with Lawful Interception, Not for Assisting in Unlawful Surveillance

A. The Responsibilities of Communications Service Providers

Under our nation's electronic surveillance laws, communications service providers have a dual responsibility: to assist government surveillance and to protect the privacy of their subscribers. Without the service providers' cooperation with lawful surveillance requests, it would be much more difficult for the government to listen in when terrorists communicate. Without the carriers' resistance to unlawful surveillance requests, the privacy of innocent Americans' communications would be threatened by zealous officials acting on their own perception, rather the law's definition, of what is right and wrong.

Accordingly, FISA created -- and Congress should preserve -- a system of incentives for corporate assistance with lawful surveillance requests and disincentives for assistance with unlawful requests. This system includes immunity and compensation for expenses when cooperating with lawful surveillance and damages liability when carriers conduct unlawful surveillance.

B. Retroactive Immunity Would Undermine the Structure of FISA

DNI McConnell has implied that companies that cooperated with the so-called Terrorist Surveillance Program violated FISA and are therefore exposed to ruinous liability. He has called on Congress to retroactively immunize the companies.

In many respects, the question of retroactive immunity is premature. Congress could safely do nothing on this issue. The cases against the companies are dealing with procedural issues and it will be several years before there is a judgment on the merits.

More importantly, retroactive immunity would be inconsistent with the structure and purpose of FISA. FISA was intended to provide clarity to both communications companies and government officials. Retroactive immunity would undermine the role the communications carriers play in effectively checking unlawful surveillance. It would place all carriers in an impossible position during the next crisis. If the government approached them with a request for surveillance that did not meet the statutory requirements, they would be uncertain as to whether they should cooperate in the hope that they would later get immunity. A communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused.

Liability for unlawful surveillance is crucial to the exclusivity of FISA. If the carriers who cooperated with the unlawful aspects of the TSP are forgiven for violating the law, then FISA becomes optional, for every time in the future that an Attorney General asks service providers to cooperate with surveillance not permitted by FISA, they may do so in the hope and expectation that they will provided immunity if found out.

C. A More Effective and Balanced Approach to Immunity

Retroactive liability is necessary for the FISA system to function properly in the future. But ruinous liability is not. Under FISA, any person other than a foreign power or an agent of a foreign power who has been subjected to unlawful electronic surveillance is entitled to recover at least liquidated damages of $1,000 or $100/day for each day of violation, whichever is greater. 50 U.S.C. Section 1810. If the conduct of the TSP was illegal, it could have affected millions of Americans, resulting in very large aggregate damages. The simplest and fairest solution would be to impose a cap on damages. However, until the facts about this warrantless surveillance program are publicly known, we urge Congress to defer any action in response to the request for immunity. Congress should not retroactively change the rules on conduct that has not been fully explained to it or to the public.

To reinforce the exclusivity of FISA, the immunity provisions of FISA and Title III should be clarified to condition communications service provider immunity on receipt of either a court order or a certification from the Attorney General that the surveillance meets a statutory exception specified in the certification.

D. Security and Privacy Concerns with the Technology of Compliance

There are enormous risks in the technical details of how communications service providers cooperate with government surveillance. In the absence of legislative guidance, the government and communications service providers are likely to conduct secret discussions to make compliance easy for both the companies and the government. This may entail installation of special software or hardware in service provider switching and storage facilities or other changes in communications networks. Congress cannot ignore this aspect of FISA, however it is amended. As computer security experts have noted, changes to communications networks intended to facilitate government interception can create vulnerabilities that can be exploited by hacker, other criminals, or foreign adversaries and could have other unintended negative consequences for privacy and security.

E. Additional Elements of Accountability

In recent years, there have been numerous problems with the Executive Branch's implementation of intelligence gathering powers. A number of these problems came to light only as a result of Inspector General audits. Earlier this year, for example, a Congressionally-mandated study by the DOJ Inspector General documented misuses of the

National Security Letter authority. The report laid out problems that the Attorney General had previously denied existed, even after he had been internally informed of them.

Congress should heed these lessons and include in any FISA legislation a charge to the appropriate Inspectors General to conduct periodic audits to measure the extent to which communications with persons in the United States are being intercepted without a particularized court order, and to assess whether the government is properly seeking a FISA court order when activities targeted at persons overseas are infringing on the rights of Americans. The Inspector General audit could also assess the adequacy of NSA's selection and filtering techniques, to determine how often surveillance targets reasonably believed to be abroad turn out to be in the United States.

The results of the audit should be reported to the House and Senate Intelligence and Judiciary Committees.

IV. The Original FISA Required a Warrant for Some Communications To and From People in the US; The "Radio Exception" Is Not a Proxy for Excluding all Communications To and From the US

The Administration claims that the PAA restores FISA to its original purpose. It claims to find this purpose both in FISA's language and in the history of the development of global communications networks over the past 30 years. Upon examination, the Administration's claim appears to be made of whole cloth. It finds no support in the text of FISA, in its legislative history, or in the history of the development of telecommunications networks.

A. The Text of FISA Does Not Show An Intent to Exclude All Foreign-to-Domestic Calls Unless a Person in the US Was Being Targeted

When FISA was adopted, it did not apply to the interception in the US of radio signals (including satellite transmissions of telephone calls) unless all parties to the radio communication were in the US or the government was intentionally targeting a particular known US person located in the US. The Administration takes a very odd view of this treatment of radio communications, claiming that it was really an exception for all communications between Americans and people abroad:

Congress designed a judicial review process that would apply primarily to surveillance activities within the United States where privacy interests are the most pronounced and not to overseas surveillance where privacy interests are minimal or non-existent. Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," the term that identifies those government activities that fall within the scope of the statute and, by implication, those that fall outside it. Congress established this dichotomy by defining "electronic surveillance" by reference to the manner of the communication under surveillance -- by distinguishing between "wire" communications -- which included most of the local and domestic traffic in 1978 -- and "radio" communications -- which included most of the transoceanic traffic in that era.

Based on the communications reality of that time, that dichotomy more or less accomplished the Congressional purpose, as it distinguished between domestic communications that generally fell within FISA and foreign international communications that generally did not.

This is a strange reading of FISA and is completely refuted by the fact that FISA in 1978 required warrants for interception of wire communications into and out of the US without regard to who was being targeted. If Congress had really wanted to exempt all calls to and from the US, it could easily have said so. As Mr. Wainstein's comments imply, and as we explain below in a little more detail, in 1978 some domestic calls were carried in part by radio (satellite and microwave) and some international calls went on wire (undersea cable). It would be odd if Congress, after years of debate in the 1970s leading to the enactment of FISA, settled for a law that "more or less" accomplished its purpose by using a wire-radio distinction as a proxy for the much more direct international versus domestic distinction that the Administration wants to find to support the PAA.

B. In 1978, Some International Communications Were Carried By Wire, and Some Domestic Calls Were Carried by Radio

The Administration tries to bolster its argument that the "radio exception" was a proxy for an international communications to and from persons in the US by claiming that it matched the topography of international communications. DNI McConnell has argued:

When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

History does not bear this out: In 1978, many international calls were carried by wire and many domestic calls were carried in part by radio. A cursory review of the history of communications technology reveals that, in 1978, (1) both cable and satellite were being used for international communications into and out of US and (2) both cable and satellite were being used for domestic-to-domestic communications. In terms of relative volume, there was certainly an ebb and flow. Throughout the 1960s and 1970s, AT&T installed a network of transoceanic cables to carry telephone and other communications, and until 1965, essentially all telephone communications international and domestic were carried by wire. The first Intelsat satellite for international telephone went up in 1965, offering better speed and lower cost, but the industry continued to lay undersea cable. AT&T laid its 6th major undersea cable to Europe in 1976, when debate over FISA began in earnest, and it completed its 7th major trans-Altantic cable in 1978, the year FISA was adopted. Meanwhile, satellites were also being deployed and used for domestic-to-domestic calls: the first Comstat satellite for long-distance domestic calls went up in 1974. Satellites may have carried a majority of international calls in 1978, but they clearly did not carry all. The trend reversed itself again in 1988, when the first fiber optic cable was laid under the Atlantic, although satellites have improved too and continue to this day to carry a substantial amount of telephone traffic.

James Baker, former head of OIPR, summed up the history in his testimony last week to the House Intelligence Committee:

With respect to the historical record, I've been looking at some documents lately, just in a preliminary manner, that seem to indicate that trans-oceanic communications were made in relatively large quantities by both satellite and coaxial cables underneath the sea, that both kinds of systems were expected to continue in service for many years and, indeed, that the use of fiber optics was already anticipated for undersea cables.

C. Was the "Radio Exception" a Foreign-to-Foreign Exception?

There is one simple explanation for FISA's radio exception: The NSA's antennae in the US were used to intercept foreign-to-foreign communications. Further research may be useful. In 1978, did foreign-to-foreign communications transit the US via satellite connections into and out of US ground stations. It seems clear that NSA's facilities in the US have long had various capabilities to intercept radio signals to and from various points around the world. The diversity of these signals intelligence activities was too complex - and perhaps too sensitive -- for Congress to spell out in legislation. But by "exempting" radio, Congress may have been trying to make it clear that the interception on US soil of foreign-to-foreign communications did not require court order.

D. The Radio Exception Was Meant to Be Temporary, Not to Become the Rule for All Technologies

In the final analysis, arguments about the legislative intent of FISA must yield to considerations about what is right today to protect both the national security and the rights of Americans.

It is clear from FISA's legislative history that Congress intended to consider subsequent legislation to regulate interception of radio communications. The Senate Judiciary Committee's 1977 report on FISA, Rept 95-604, states:

"The reason for excepting from the definition of 'electronic surveillance'
the acquisition of international radio transmissions, including international
wire communications when acquired by intercepting radio transmission
when not accomplished by targeting a particular United States person in the United States, is to exempt from the provisions of the bill certain signals intelligence activities of the National Security Agency.

Although it is desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that, except when they target particular United States citizens or resident aliens in the United States, they should be considered separately by the Congress. The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities." P. 34 (emphasis added).

"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. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely during the interim period when the activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed." P. 64 (emphasis added).

V. In a Major Change, the PAA Appears to Authorize Warrantless Acquisition of a Wide Range of Stored Communications

It is impossible to tell whether the PAA is very cleverly drafted or very carelessly drafted. In truth, it is probably some of both. It is clear that the statute is subject to multiple interpretations. There has been considerable debate about whether it encompasses various privacy intrusions - physical searches, access to business records, interception of domestic-to-domestic communications -- going beyond communications surveillance of international communications.

This concern grows out of the decision to base the PAA around a provision that says, in Alice-in-Wonderland fashion, that certain forms of electronic surveillance are not "electronic surveillance," thereby upsetting a very complex statute that contains many authorities and restrictions keyed to the definition of "electronic surveillance." It is compounded by the unwise use at the beginning of Section 105B of the phrase "Notwithstanding any other law. ... ." It also is compounded by the inconsistent use of undefined terms like "directed at" and "concerning."

The Administration has sought to dampen these fears, but it is apparent that the PAA does not establish clear rules for intelligence activities that the Administration says are of utmost importance to the national security. The goal of FISA was to provide certainty to intelligence agency personnel working under pressure. The PAA undermines that goal.

In at least one respect, it does appear that the PAA - intentionally or unintentionally -- authorizes a new form of government access to communications, including possibly domestic-to-domestic communications. This new authority concerns access to stored communications.

When FISA was enacted, almost all electronic communications were ephemeral: if they were not captured in real time, they were gone. Among the many consequences of the digital revolution and the rise of the Internet is something CDT calls the "storage revolution." Huge quantities of our email are stored on the computers of service providers, often for very long periods of time. With the advent of voice over IP services, the storage of voice communications may also become more common. See CDT's report "Digital Search & Seizure" (February 2006) http://www.cdt.org/publications/digital-search-and-seizure.pdf.

Stored communications are covered by the Stored Communications Act, part of the Electronic Communications Privacy Act of 1986. It is unclear how stored communications fit within the FISA framework. FISA's definition of electronic surveillance is limited to the acquisition of communications "by an electronic, mechanical, or other surveillance device." If an email service provider accesses the stored communications of its subscriber, copies them and sends them to the government, is that the use of "an electronic, mechanical, or other surveillance device?" If it is not, then the acquisition of those stored communications is not electronic surveillance. And if something is not electronic surveillance, then the powers of Section 105B are available.

Section 105B added by the PAA creates a powerful mechanism for the government to force communications service providers (and maybe others) to cooperate with the government's acquisition of stored communications without court approval. Section 105B expressly applies to communications "either as they are transmitted or while they are stored" and to "equipment" that is being used to store communications. While Section 105A exempts from FISA any surveillance that is directed at targets believed to be abroad, Section 105B empowers the Attorney General, without a warrant, to compel service providers to cooperate with the acquisition of foreign intelligence information concerning persons believed to be abroad. Section 105B applies not only to communications exempted from FISA by virtue of Section 105A, but to other means of "acquisition" of communications that are not electronic surveillance. Information may "concern" a person abroad even if it is in the communications of a US person. Probably every email from the New York Times Baghdad bureau to editors in New York contains foreign intelligence concerning persons outside the US. If the disclosure of email by a service provider is not "electronic surveillance," then the PAA creates a major new authority. The language that introduces Section 105B - "Notwithstanding any other law" - would seem to override the Stored Communications Act or any other law on access to stored email. At the very least, this is an issue to be explored and clarified.

Conclusion

The ambiguous language of the PAA presents several unanswered questions, notably -

? Which agencies can exercise the new authority? There seems to be no limit on the agencies to which Section 105B authority can be granted. In the past, E.O. 12333, which is being rewritten, has limited which agencies could perform electronic surveillance, but the PAA carves certain acquisitions of communications out of FISA's definition of electronic surveillance. It is impossible to predict what relationship the Administration will define between the PAA and the new E.O. on intelligence activities, but many agencies could have the power to compel service provider cooperation with acquisition of communications.
? What persons can orders be served upon? Under Section 105B(e) of the PAA, the Director of National Intelligence and the Attorney General may direct any person to provide the government with assistance. Compare this with 50 U.S.C. 1802(a)(4). Under the PAA, the certification compelling cooperation need not be addressed to the service provider as an entity, but could be directed to an individual employee, suggesting that the acquisition of communications could occur without the knowledge or oversight of the senior management of the service provider.
? What communications can be acquired? It is clear that the PAA applies to real-time communications and it is pretty clear that it applies to stored email. What about the communications that occur daily as part of the global airline reservation system, which contain foreign intelligence concerning persons outside the US? What about Electronic Funds Transfers and other inter-bank communications? Every time a credit card is read at a point of sale, there is a communication between the point of sale and the credit card network, indicating essentially where the credit card holder is and what he is doing. Are these communications covered? Are the credit card companies providers of communications services to themselves and the merchants who accept the cards?

In the new environment of global communications networks, and in light of the threat of borderless terrorism, it is likely that the NSA is acquiring and disseminating significantly larger quantities of conversations to which a US person is a party. As more information about citizens and other US persons is being relied upon to make decisions directly affecting individuals, checks and balances are needed at each step of the process. The legitimate goal of providing the NSA with speed and agility in targeting persons overseas can be accomplished in a way that builds on the constitutional system of judicial review. The Center for Democracy and Technology looks forward to working with the Committee to achieve that objective.

1 In his 2005 confirmation hearing, General Hayden said "it is not uncommon for us to come across information to, from or about what we would call a protected person--a U.S. person." http://www.fas.org/irp/congress/2005_hr/shrg109-270.pdf p. 20. In its "Transition 2001" report, completed in December 2000, the NSA concluded, "The National Security Agency is prepared ... to exploit in an unprecedented way the explosion in global communications. This represents an Agency very different from the one we inherited from the Cold War. It also demands a policy recognition that the NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist." (Emphasis added.)

2 See United States v. Ozar, 50 F.3d 1440, 1448 (8th Cir. 1995), cert. denied, 116 S.Ct. 193 (1995) (upholding the "two minutes up/one minute down" technique recommended by the Justice Department, in which FBI agents listened to two out of every three minutes of every phone conversation).

3 "I could agree to a procedure that provides for court review -- after needed collection has begun -- of our procedures for gathering foreign intelligence through classified methods directed at foreigners located overseas. While I would strongly prefer not to engage in such a process, I am prepared to take these additional steps to keep the confidence of Members of Congress and the American people that our processes have been subject to court review and approval." Statement by Director of National Intelligence, Subject: Modernization of the Foreign Intelligence Surveillance Act (FISA), August 2, 2007 http://www.cdt.org/security/nsa/dnistm82.pdf.

4 There seems to be a drafting error in the PAA. The new Section 105B(a)(1) states that the court shall review pursuant to Section 105C procedures for determining that acquisitions of foreign intelligence under Section 105B concern persons reasonably believed to be outside the US, but Section 105C only requires the Attorney General to submit to the court and the court to assess procedures by which the government determines that acquisitions under Section 105B do not constitute electronic surveillance.

5 http://www.msnbc.msn.com/id/7614681/site/newsweek/. The practice came to light most recently when U.N. ambassador nominee John Bolton explained to a Senate confirmation hearing that he had requested that the names of U.S persons be unmasked from NSA intercepts on 10 occasions when he was at the State Department.

6 Eric Lichtblau and Scott Shane, "Files Say Agency Initiated Growth of Spying Effort." New York Times, January 4, 2006. In the context of court-authorized surveillance, this may have been appropriate. For a discussion of the dissemination of identifying information, see the recommendation on "authorized use" in the Third Report of the Markle Task Force on National
Security in the Information Age. It is unclear whether the Administration intends to apply these same liberal dissemination rules to information acquired under the PAA, which is likely to result in an increase in the collection of information identifying US persons.

7 Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr, "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," New York Times (January 17, 2006).

8 Ellen Nakashima, "Terrorism Watch List Is Faulted For Errors," Washington Post September 7, 2007 at p. A12. The IG report is at http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

9 "[W]e have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated. ... These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities. Testimony of DNI J. Michael McConnell before the House Permanent Select Committee on Intelligence, September 20, 2007 at p. 12.

10 Susan Landau, "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," Washington Post, August 9, 2007, p. A17 http://www.washingtonpost.com/wp-dyn/content/article/2007/08/08/AR2007080801961.html.

11 Prepared Remarks of Kenneth L. Wainstein, Assistant Attorney General for National Security, on FISA Modernization at the Georgetown University Law Center's National Security Center, September 10, 2007 http://www.usdoj.gov/opa/pr/2007/September/07_nsd_699.html.

12 Testimony of DNI J. Michael McConnell before the House Permanent Select Committee on Intelligence, September 20, 2007 at p. 5