Testimony of

Bryan Cunningham

September 25, 2007

KEEPING THE FISA BALANCE. PROTECTING US FROM ATTACK
Statement of
H. BRYAN CUNNINGHAM1
PRINCIPAL, MORGAN & CUNNINGHAM LLC
www.morgancunningham.net
Former CIA Assistant General Counsel and Federal Prosecutor (1994-2000)
Deputy Legal Adviser to the National Security Council (2002-2004)
Information Security and Privacy Lawyer (2004-Present)
before the
UNITED STATES SENATE COMMITTEE ON THE JUDICIARY
On the subject of
"STRENGTHENING FISA: DOES THE PROTECT AMERICA ACT PROTECT AMERICANS' CIVIL LIBERTIES AND ENHANCE SECURITY?"
September 25, 2007

Mr. Chairman, Ranking Member Specter, and Members of the Committee, thank you for inviting me to testify again before this Committee on one of the most important national security challenges facing our Nation. Shortly after disclosure of the Terrorist Surveillance Program, I co-authored, with former senior Democratic homeland security staff member Dan Prieto, an Op-Ed entitled "The Eavesdropping Debate We Should Be Having" (http://www.ksg.harvard.edu/ksgnews/Features/opeds/020506_prieto.htm). We called for three touchstones for foreign intelligence surveillance: (1) updating FISA to achieve its original national security and civil liberties goals, but adjusting the badly outdated law to the revolutionary technological since 1978 so that our intelligence officers can protect us from attack; (2) ensuring that equally strong civil liberties protections, though perhaps different from those envisioned in 1978, are built into any such changes; and (3) continuing a meaningful role for our Courts to the extent consistent with our Constitution and national security.

The Protect America Act (PAA), passed by Congress last month, met these three goals to a significant degree, at least in the area of collection of intelligence from foreign-to-foreign communications. This hearing, and others that have preceded it, are an important part of that debate we recommended 19 months ago and I commend this Committee for furthering it.

As a recovering career government attorney and intelligence officer (having served six years in the Clinton Administration and two years in the George W. Bush Administration), I will do my best to resist the temptation to slip into a legalistic discussion of the minutae of the Foreign Intelligence Surveillance Act or the related constitutional issues. To assist this Committee, of course, our panel likely will have to get into these some of these details today, but first I would like to take a step back. Unfortunately, some of the loudest voices in this debate over the past few weeks have generated far more heat than light. There has been a great deal of misunderstanding, if not misinformation, in the public discussion, and I hope we can today dispel some of the myths that have arisen since Congress passed the PAA.

I would like to provide a couple of observations and offer several recommendations and I will be pleased to respond to any questions the Committee may have, or to provide additional information as the Committee may request.

The FISA Balance

For the first two centuries of our Nation's history, our courts uniformly recognized that our Constitution assigned to the Executive Branch of our government, and specifically the President, the "plenary" authority over the conduct of our foreign affairs.2 For example, in Department of the Navy v. Egan, Justice Harry Blackmun, writing for the majority, reiterated that the "Court . . . has recognized 'the generally accepted view that foreign policy was the province and responsibility of the Executive.'"3 More to the point, Justice O'Connor stated in 1988 that the Executive Branch's authority to conduct intelligence operations "lie[s] at the core of "the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations."4

Prior to 1978, all presidents, of both political parties, at least since Franklin Roosevelt, conducted significant programs of foreign intelligence electronic surveillance, here and abroad, targeted against Americans and foreigners, without warrants or other court involvement. Federal appellate courts repeatedly upheld the constitutionality of such warrantless surveillance.5 To cite one example, the Fifth Circuit Court of Appeals, in United States v. Brown, upheld the President's inherent constitutional authority to authorize warrantless wiretaps for foreign intelligence purposes, explaining that:

[B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, we reaffirm. . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence. Restrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere. Our holding . . . is buttressed by a thread which runs through the Federalist Papers: that the President must take care to safeguard the nation from possible foreign encroachment, whether in its existence as a nation or in its intercourse with other nations.6

Following revelations about real "domestic spying" (in stark contrast to what we are discussing today which, based on United States Supreme Court and other federal court precedent, is foreign intelligence collection) in previous decades, in the late 1970s Congress and Administrations of two presidents of different political parties set out to regulate - by statute - electronic surveillance for foreign intelligence purposes. During the lengthy deliberations preceding passage of that statute, both the Executive Branch and the FISA Congress itself, in legislative history, made clear that the passage of FISA did not mean either that: (1) the Constitution required the precise requirements enacted in FISA for foreign intelligence surveillance; or (2) that the Supreme Court would conclude that Congress could constitutionally bind the President to those requirements in all cases.

As recent testimony to Congress has made abundantly clear, and as the FISA Congress legislative history confirms, the balance that was struck by the 1978 Congress between protecting Americans' vital civil liberties from undue government intrusion and the equally vital responsibility to protect our people from foreign threats was essentially this: Court-issued warrants should be required to conduct electronic surveillance targeted or directed at United States Persons (citizens or Permanent Resident Aliens) located inside the United States. No such warrants, or, indeed, even court involvement, should be required to conduct such surveillance targeted or directed against individuals (including US Persons) located outside the United States.

The 1978 Congress quite clearly did not intend that warrants be required for electronic surveillance targeted against persons located outside the United States. This is evident not only from the definitions of "electronic surveillance" in FISA itself, but also from the 1978 FISA legislative history.7

I believe that most on both sides of the political aisle today believe that, generally speaking, this is the proper balance, assuming it remains technologically possible to observe these lines of demarcation, which is increasingly doubtful. As an aside, as has been discussed publicly by technically and legally knowledgeable experts, there are a host of technological developments which have rendered the original FISA unworkable against post-9/11 threats to our Nation, including the development of "packet-based" communications, the use of proxy servers and Internet-based, encrypted, highly mobile telephone communications and PDAs, the increasingly distant relationship between IP addresses and real-time, actual physical location, and the routing of vast amounts of purely overseas Internet communications through the United States.8 One key problem remains the difficulty, given today's technology, to determine before the fact who the bad guys are, where they are located, and where the bad guys they are calling are located. To cite one specific example, as Director of National Intelligence McConnell testified last week, and common sense dictates, it is today, in many cases, impossible to make a determination, in advance of initiating electronic surveillance, whether the communications of an overseas target will be purely foreign-to-foreign.

In order to put this balance into our law, the 1978 FISA Congress chose a set of understandable but, in hindsight, mistaken factors to try and carve out foreign-to-foreign communications from the law's requirements. For purposes of discussion of the PAA, the key factors in the original FISA were: (1) place of collection (whether inside the United States or overseas); and (2) method of communications (whether by "wire" or by "radio"). In 1978, the vast majority of domestic communications were carried, literally, by wire, whereas the vast majority of overseas communications of interest to our intelligence community were carried by "radio," including by satellite. Thus, it made sense in 1978 to apply FISA's strict requirements principally to wire communications but not to "radio" communications. Clearly demonstrating Congress' intent to exempt from FISA's coverage collection of foreign-to-foreign communications even when the collection was conducted inside the United States, the law only applied its strict requirements to collection against radio communications "if both the sender and all intended recipients are located within the United States" (or, of course, if the communications of a particular, known US Person located in the United States were intentionally targeted).9

The key historical point, seemingly lost in much of the debate, is this: selection of these statutory criteria were the means to an end, not an end in themselves. And the means no longer further the original end. This is because, gradually over the three decades since FISA was passed, the 1978 communications technology situation reversed itself. Today, a significant percentage of truly domestic U.S. communications are carried by "radio," cellular and microwave transmissions, while most international communications now are carried by "wire," that is, fiberoptic cables.

As a result, prior to the PAA, as one FISA Court judge reportedly ruled earlier this year, FISA had morphed far beyond the intent of Congress to require a warrant even for communications between two foreigners both overseas so long as the collection happened to occur in the United States. This clearly was not the balance that the 1978 Congress intended to strike.

Part of the bargain that the 1978 Congress understood, as have all subsequent Congresses under the control of both political parties, was that electronic surveillance of foreign-to-foreign communications, and, indeed, some communications between targets abroad and the United States, would be carried out with no warrant and no judicial involvement whatsoever. Such surveillance was carried out effectively, and consistent with the Fourth Amendment, for nearly three decades, under Executive Orders and strictly enforced procedures required by those orders. Also understood by the 1978 Congress, and all subsequent Congresses, was that, in the course of targeting the communications of foreigners abroad, our government would necessarily also collect a significant amount of communications of individuals in the United States with whom the overseas targets were communicating. Fourth Amendment protection for Americans under these circumstances was achieved by a panoply of strict requirements, including: Attorney General approval for collection, though overseas, targeting US Persons abroad; careful training, monitoring, and oversight; strict limitations on sharing and use of such information; and, perhaps most important, strictly enforced minimization requirements for information related to US Persons.

Through these minimization requirements, as with domestic criminal wiretaps, information not targeted for collection and not meeting the criteria of information authorized for collection ("foreign intelligence" in the case of foreign intelligence collection), or mistakenly collected, generally could not be shared, used, or retained by the government. Based on recent testimony, it appears that equivalent protections are in place or being developed for information to be collected under the PAA. Under the PAA, however, unlike during the past three decades, there is some FISA Court oversight of the procedures under which such collection is undertaken, as well as enhanced Congressional oversight.

To be clear: US Government electronic surveillance of foreign-to-foreign communications outside of FISA has been conducted for decades, even though it has been well understood that communications of individuals located inside the United States would be collected - without a warrant or court involvement -- "inadvertently," where an overseas person, not the person here, was targeted. This is not new and it is precisely the situation that appears to pertain after passage of the PAA.

Rewriting the Bargain

Although I do not know the facts, and they may be classified, it is possible that the PAA's removal of the "place of collection" limitation under FISA will increase the amount of "inadvertent," non-targeted collection of communications of persons located in the United States communicating with targeted suspected terrorists overseas or other foreign intelligence collection targets. The PAA, by its explicit terms, however, only modifies the warrant requirement for electronic surveillance targeted against persons "reasonably believed to be located outside the United States," and the law contains not a word about electronic surveillance targeted against persons located here. Nonetheless, PAA opponents have repeatedly asserted that "millions" or "billions" of communications of persons located here will now be collected that were not collected prior to the PAA. Since, as discussed above, the same types of communications involving persons inside the United States have been inadvertently collected for decades under only Executive Orders, and in the absence of any other plausible explanation, I can only guess that it is an assumption of additional volume of such communications given the removal of the place-of-collection restriction that has led to such charges.

If this is in fact a principal objection of the PAA's opponents, it may be a legitimate issue for debate, but opponents should straightforwardly explain what they are attempting to do: they are attempting to rewrite the bargain, to upset the balance, struck by the 1978 FISA Congress. That "bargain" was, again, to require warrants for electronic surveillance targeted against persons in the United States and not for those outside it. Place and type of collection limitations were nothing more or less than the means to enforce that bargain. If opponents want to argue that the American people should rewrite that bargain, should undo the balance struck decades ago under continuing threat of catastrophic foreign attack, they should say so. That may be a legitimate debate. It is not, in my view, legitimate or helpful to suggest, as many have, that somehow the government is grabbing sweeping new powers to "spy on" Americans at home. Quite the opposite. What the PAA really did was to carry forward the bargain, to restore the balance between civil liberties and protection from attack so carefully struck in 1978. If we want to reconsider that balance in wartime, Congress should least be clear that that is what it is doing.

Public Confidence, Unintended Consequences, and Clearing Smoke

Viewing the Protect America Act in its proper context, however, is not to say that it cannot be improved upon. There are a number of measures which, while not, in my view, constitutionally necessary, could increase congressional and public confidence, provide permanent, clear guidance to the civil servants carrying out intelligence collection, and increase the effectiveness of whatever program ultimately is made permanent. In addition to the proposals discussed at the end of my testimony, areas where improvements potentially could be made include:
More clearly defining, and possibly strengthening, the role of the Foreign Intelligence Surveillance Court, in approving, and supervising the use of, the criteria and parameters for PAA-authorized collection;
Providing more comprehensive immunity for private sector communications service providers assisting the government in carrying out electronic surveillance activities where those providers are informed, in writing, of the lawful authority under which they are asked to act; and
Clarifying, whether in statute or legislative history, the definitions of some of the terms used in the Protect America Act, potentially including "targeted," "directed," and "concerning"

Such changes, however, should only be made after careful consideration of their potential unintended consequences, and specific language should be proposed early in the process to give all sides time to fully understand its implications. Further, any such changes must take into account all legitimate needs, arguments, and explanations of those technically expert in the area and, critically, those who must carry out the law's requirements, even if some of those arguments and explanations may not be discussed publicly. Finally, and most importantly, any changes must be made in light of cold, clear facts and a realistic understanding of the history and constitutional status of electronic surveillance in the United States, and of the original FISA. Decisions should not be made based on misleading, false, or speculative arguments, about, for example, "billions" of new communications of individuals in the United States, or "domestic spying," or be based on partisan political battles or ill will between the current Congress and the current Administration. After all, if Congress gets it right, the new methods for carrying forward the old balance will likely stand for many years, and will almost certainly be used far more by future presidents, of both political parties, than by the current one.

Private Sector Cooperation and Risk Aversion

Once again, I want to commend the Chairman and Senator Specter and those in Congress attempting to foster a sober, fact-based debate on how to strike the right balance between protecting against attack and safeguarding our

civil liberties. As I argued in my 2006 Op-Ed, Congress is the appropriate place for this debate and I am pleased to be a part of it, along with the other members of this panel. The debate must be thorough and vigorous. But, in my view, it should be fought here, in Congress.

Unfortunately, it is being fought in our courts and the media as well and, to dramatically understate the problem, not always based on accurate information. Recent government testimony indicates that FISA modernization opponents, because they object to the government's actions, have filed more than 40 civil lawsuits including, disturbingly, against communications providers alleged to have assisted the government in conducting electronic surveillance activities, even where the government allegedly assured such providers that requests for assistance were lawful and constitutional. Political differences about activities to protect our Nation from attack should not be fought through proxy attacks on companies simply trying to assist in defending our country. Providers should be able to rely on assurances from their government and should not be retroactively saddled with economically punishing litigation as a way to try and prevent them from cooperating with the government.

Such attacks are bad public policy. Speaking as a private lawyer advising companies on their interaction with the government, I believe that attempting to settle political or policy differences through such proxy lawsuits succeeds only in creating uncertainty and a reluctance on the part of the private sector to cooperate with the government, even where the law is clear. I also, frankly, think it is fundamentally unfair, if not immoral, to try, through litigation punishing those cooperating with the government, to intimidate service providers and, thereby, win political fights that rightfully belong in Congress.

Multiple bipartisan investigations criticized, appropriately in my view, both the Clinton and Bush Administrations for risk aversion by multiple intelligence agencies, and for failing to utilize their full legal authorities to collect intelligence, including through wiretapping, concerning communications between terrorists overseas and their confederates here in the United States.10 Having spent a number of years in the Clinton Administration as CIA Assistant General Counsel advising career officers conducting risky intelligence operations, I saw firsthand how well-founded fears of career-ending investigations and after-the-fact legal and rule changes led dedicated officers to fail to take clearly lawful and proper actions to collect intelligence. This risk aversion, which crippled our Nation before 9/11, is, I fear, returning to the ranks of our career civil servants in the intelligence and law-enforcement officers.

Legitimate oversight is a necessary and vital part of our democratic system and, of course, intentional illegal activity must be discovered and punished. But our career intelligence officers - and, make no mistake, these are the people, not the President, the Vice President, or other political appointees, who must carry forward whatever vital reforms Congress enacts - must not be put into the position of attempting to do their duty under the constant fear of being punished for following rules that have been changed. Among other things, this means putting into place legal rules that are: (1) clear and easy to follow; and (2) stable over some reasonable period of time. In short, government by sunset cannot become the norm in the regulation of intelligence activities to protect our country from attack. Our career officers need to know that the rules will be the same next year as this year, absent significant changes in technology, threats, or other compelling conditions.

In addition to doing right by our career officers and reducing risk aversion, stable legal rules over a reasonable period of time are the only workable solution. Each time the law changes significantly, policies, regulations, other guidance must change, and, perhaps most importantly, massive changes must be made to numerous and comprehensive training programs in order to reeducate generations of officers conducting intelligence activities. Whatever Congress does next in the vital area of FISA modernization, I urge you to satisfy yourselves with the balance struck sufficiently to make those changes permanent. Wherever the political blame may fall, six-month sunsets are bad for morale, bad for the risk taking necessary for successful intelligence collection, and dangerous to our ability to protect our Nation from attack.

Potential Solutions Beyond the Protect America Act

As noted above, the PAA, whether one supports it as passed or not, only solves one of the myriad problems created by technological change and the language of the original FISA. Other challenges which, in my view, require urgent attention, include: collection of information originally sought under the Terrorist Surveillance Program; collecting foreign intelligence in situations where there is literally not time to get any new advance approval without missing

critical threat information, or no way to timely determine place of collection, location, or nationality of the targeted individual; and protecting privacy and civil liberties when information collected with electronic surveillance and other highly intrusive techniques is shared across entities and governments. These challenges, in my view, can only be addressed adequately by some combination of the approaches discussed below. These approaches also, in my judgment, can help improve the PAA, and its implementation going forward.

Programmatic Judicial Review and Approval

In our February 5, 2006, Op-Ed, Daniel Prieto and I recommended that Congress and the President, in modernizing FISA:

Ensure a role for the courts. To preserve and promote appropriate judicial oversight, new methods of court involvement must be considered. As one example, courts could pre-approve categories of electronic surveillance. This would allow the government to apply strict, pre-determined criteria to particular communications without the need for case-by-case court approvals. Categories, criteria and eavesdropping activity would be subject to regular re-examination, with approvals subject to periodic court renewals.

S. 2453, proposed in 2006, would have created clear jurisdiction for the Foreign Intelligence Surveillance Court (FISC) to conduct just such "programmatic" review. As such, I supported that legislation, even for targeted collection of international terrorism-related communications. Though I do not believe such judicial involvement to be constitutionally required, at least for communications targeted at persons located overseas, Congress should examine - based on independent expert factual analysis - whether our ability to timely determine location has become so weak that location can no longer be a meaningful factor in most cases. If that is so, as has been suggested by many experts, programmatic review, regardless of location, merits much more consideration.

Such review would provide meaningful judicial oversight, likely consistent with the Fourth Amendment for foreign intelligence-related surveillance, while redressing what I believe to be one of the fatal flaws of the 1978-era FISA in today's world, namely the requirement for individualized, target-by-target approval, based on known facts which often, in the post-9/11 world, will be unknown in any timely fashion, and perhaps unknowable given the technology and enemies we now face.

Any legislative mandate for such "programmatic approval" by courts, however, should consider whether specifically articulated criteria for the application for, and granting of, applications for programmatic surveillance orders might be useful. Any such legislation should include a clear explanation, probably in legislative history, of Congress' views as to how the articulated criteria, if met, satisfy the requirements of the Fourth Amendment.

Machine Triage/Electronic Tracking

In my view, we urgently need a recognition in law, with concomitant adjustments in the law, that the vast majority of the government's "surveillance" in the future will (if it does not already) actually consist of what I call "machine triage," that is, review of data by computers and selection of information for review by humans based on selection criteria meeting legal standards appropriate to protect our civil liberties. S. 2453, in the previous Congress, recognized the concept of "electronic tracking," as "the acquisition by an electronic, mechanical, or other surveillance device"11 of certain electronic communications. The draft legislation appeared to recognize such tracking as an integral part of an electronic surveillance program eventually leading to access by human beings to a far smaller number of selected communications than those triaged by computer. This distinction, between information "seen," or processed only by machine, and information reviewed by a human government is, in my judgment, crucial, and as technology continues to evolve, one with which our electronic surveillance laws must grapple.

I believe that the use of machines to triage communications content and other sensitive, i.e., personally identifiable, information prior to human review will be crucial over the coming years in balancing privacy and civil liberties and our national security. Depending upon one's interpretation of the current FISA, such "machine triage" - the use of which bi-partisan experts, including the Markle Commission Task Force, have recommended - might today still require individual FISA applications. Such a situation, obviously, would present an insurmountable obstacle to the use of

machine triage that could enhance civil liberties and operational capabilities by reducing dramatically the volume of information that must be reviewed by our perennially resource-starved intelligence agencies.

Technology to Improve Our Ability to Prevent Attacks While Enhancing Civil Liberties

As has been widely discussed, by Markle and others, currently available technologies can dramatically enhance both the government's ability to utilize increasingly large amounts of data and do so in a way that better protects our privacy and civil liberties. Congress took a significant step forward on this front in the recently signed bill to enact the 9/11 Commission's recommendations. In that new law, Congress mandated that the Executive Branch build into the emerging Information Sharing Environment technologies, available today, that:
permit analysts to collaborate both independently and in a group (commonly known as "collective and noncollective collaboration"), and across multiple levels of national security information and controlled unclassified information;
provide a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and
incorporate continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.12

As these new legal requirements begin to be met, as they can be with current technology, privacy and civil liberties protections not technologically possible several years ago can become routine parts of our government's activities. Equally important, as analysts and operators become far more productive, collaborative and, hopefully, effective at their missions, it may become possible for the government to do far more with far less information.

Conclusion

Today continues a vitally necessary debate, in the place where it should occur, the United States Congress. The PAA, while capable of improvement, is an important step forward in protecting our country while modernizing our privacy and civil liberties protections, and should be made permanent. Modernization reforms, however, must also take place in other areas of foreign intelligence collection, along the lines, and utilizing available technologies to achieve the new legal requirements, discussed herein. I remain confident that the appropriate balance between protecting our Nation from attack and guarding our privacy and civil liberties can, and will, be struck, so long as our career officials remain able to do their jobs and leaders on all sides of the debate go forward expeditiously, based on accurate information, and in good faith. I thank the Committee for inviting me to be part of that debate.

1 As additional relevant experience, I am currently a Principal at the Denver law firm of Morgan & Cunningham LLC, practicing primarily in the areas of information security and privacy. www.morgancunningham.net I was a founding vice-chair of the ABA CyberSecurity Privacy Task Force, and, in January 2005, was awarded the National Intelligence Medal of Achievement for work on information issues. I serve on the National Academies of Science Committee on Biodefense Analysis and Countermeasures and am a member of the Markle Foundation Task Force on National Security in the Information Age. The views expressed in my testimony are entirely my own.

2 "The preservation of our territorial integrity and the protection of our foreign interests is intrusted, in the first instance, to the President. The Constitution, established by the people of the United States as the fundamental law of the land, has conferred upon the President the executive power; has made him the Commander in Chief of the Army and Navy; has authorized him, by and with the consent of the Senate, to make treaties, and to appoint ambassadors, public ministers, and consuls; and has made it his duty to take care that the laws be faithfully executed. In the protection of these fundamental rights, which are based upon the Constitution and grow out of the jurisdiction of this nation over its own territory and its international rights and obligations as a distinct sovereignty, the President is not limited to the enforcement of specific acts of Congress. He takes a solemn oath to faithfully execute the office of President, and to preserve, protect, and defend the Constitution of the United States. To do this he must preserve, protect, and defend those fundamental rights which flow from the Constitution itself and belong to the sovereignty it created. 22 U.S. Op. Atty. Gen. 13, 25-26, Foreign Cables, (1898) (citing, inter alia, Cunningham v. Neagle, 135 U.S. 1 (1890) (emphasis added). Indeed, the founders of our republic specifically recognized the primary position of the President in the field of foreign affairs. For an excellent discussion of this history, see Powell, H. Jefferson, The Founders and the President's Authority over Foreign Affairs. William & Mary Law Review, Vol. 40, pp. 1471-1537 (May 1999).

3 484 US 518, 527, 530 (1988).

4 Webster v. Doe, 486 U.S. 592, 605-06 (1988) (O'Connor, J., concurring in part, dissenting in part) (emphasis added) (citing prior Supreme Court decisions in United States v. Curtiss-Wright Export Corp., Department of Navy v. Egan, and Totten v. United States, 92 U.S. 105 (1876)). A number of key United States appellate court decisions confirming this view specifically in the context of foreign intelligence electronic surveillance are discussed in my February 3, 2006 letter to this Committee entitled Additional Constitutional Authorities Relevant to NSA Electronic Surveillance of International Terrorist Communications and in amicus briefs I co-authored with the Washington Legal Foundation, in litigation challenging the TSP in the Eastern District of Michigan and the Court of Appeals for the Sixth Circuit. All are available at www.morgancunningham.net.

5 For one of the most thorough and scholarly publicly available discussions of the constitutionality of warrantless electronic surveillance for foreign intelligence purposes, as well as the law of national security surveillance more generally, see David Kris and Doug Wilson, National Security Investigations and Prosecutions (West 2007). The authors explain: "every court of appeals to consider the question concluded that the President has constitutional authority to conduct warrantless electronic surveillance of foreign powers and their agents in the United States; the same result would seem to apply, a fortiori, to surveillance abroad, where Fourth Amendment protections for U.S. persons are certainly no stronger than they are in this country." Id. at 16-3 (emphasis added).

6 484 F.2d 418, 426 (5th Cir. 1973) (emphasis added) (citations omitted); Accord United States v. Butenko, 494 F.2d 593, 603 (3d Cir. 1974), (noting that while the "Constitution contains no express provision authorizing the President to conduct surveillance . . . it would appear that such power is . . . implied from his duty to conduct the nation's foreign affairs"). Similarly, in United States v. Truong Dinh Hung, a case cited with approval in 2002 by the Foreign Intelligence Surveillance Court of Review, the Court of Appeals for the Fourth Circuit, in approving warrantless electronic surveillance for foreign intelligence purposes, stated the matter plainly:
Perhaps most crucially, the executive branch . . . is . . . constitutionally designated as the pre-eminent authority in foreign affairs . . . . Just as the separation of powers in Keith forced the executive to recognize a judicial role when the President conducts domestic surveillance, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.
629 F.2d 908 (4th Cir. 1980) (emphasis added) (citations omitted). The passage of FISA, and the passage of years since, in no way undermine the reasoning of the Brown court, and other authorities cited herein, as to the constitutional and practical reasoning for Presidential primacy in this area.

7 For example, the House Permanent Select Committee on Intelligence (HPSCI) report on FISA stated that the committee had "explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillance." H.R. Rep. No. 95-1283, pt. 1, at 22 (1978). Similarly, FISA's drafters made clear that the so-called "residual definition," intended to encompass types of electronic surveillance for which FISA's warrant requirement would apply, but which were not captured by the more specific definitions, was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." Id. at 52.

8 See, e.g., testimony and writings of Kim Taipale particularly his June 19, 2006 testimony before the House Permanent Select Committee on Intelligence.

9 50 U.S.C. section 1801(f)(3) and (f)(1)

10 See, e.g., Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001, at p.39

11 Emphasis added.

12 Improving America's Security Act of 2007, Section 112(2). This same statute also mandates a report by the Executive Branch to Congress on the feasibility of
(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment for a

particular purpose that the Federal Government, through an appropriate process, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an `authorized use' standard); and
(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, in any cases in which--
`(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and
`(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information."
Id. at Section 112(1)(j). The policies and technologies discussed in these provisions also can significantly assist the government in establishing the proper balance between national security and privacy and civil liberties.