Volume One / January 2007

FOR THE RECORD

A PUBLICATION OF THE CENTER ON LAW AND SECURITY AT THE NYU SCHOOL OF LAW

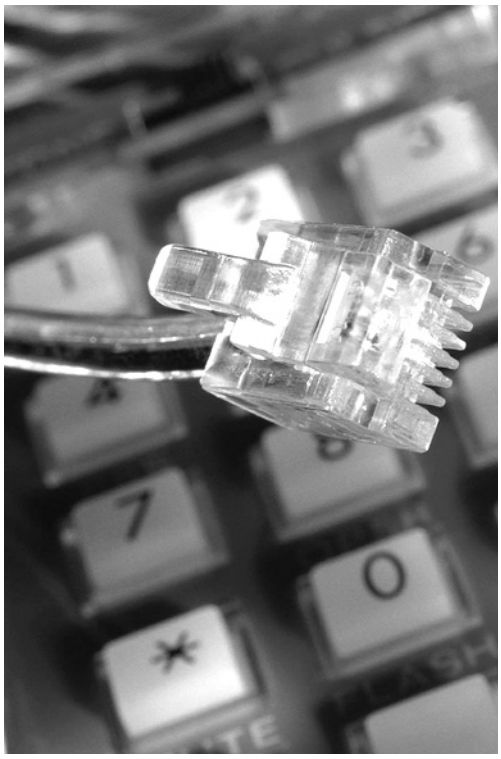
The NSA Wiretapping Program

"If somebody from al Qaeda is calling you, we'd like to know why."

President George W. Bush, January 1, 2006

"The disrespect embodied in these apparent mass violations of the law is part of a larger pattern of seeming indifference to the Constitution."

Former Vice President Al Gore on the NSA Program, January 16, 2006



Photodisc/Photodisc Blue/Getty Images

The NSA Wiretapping Program

Table of Contents:

Acknowledgements

Editor in Chief
Karen J. Greenberg

Series Editor
Michael Sheehan

Research Fellow
Paul Cruickshank

Research
Daniel Freifeld
Francesca Laguardia
Alisa Randell
Zach Stern

Editorial Advisor
Tara McKelvey

Editorial Associate
Jeff Grossman

Designer
Wendy Bedenbaugh

With special thanks to the entire staff of The Center on Law and Security

The Center on Law and Security
New York University School of Law
110 West Third Street, Suite 217
New York, NY 10012
(212) 992-8854
www.lawandsecurity.org
CLS@juris.law.nyu.edu

Editor's Introduction

The Center on Law and Security is pleased to publish its first volume of *For the Record*, a series of factual guides which will address issues central to national security and the war on terror. Port security, information sharing networks, misperceptions of the enemy and the threats posed by chemical, biological, radioactive and nuclear weapons are among the topics we hope to examine. The purpose of this series is to present an overview of relevant history, current developments, and the basic issues involved in these and other controversial matters related to the nation's security. Given the heightened partisanship of the past few years, the Center is seeking to establish the facts that lie beneath political rhetoric. Only when the public has a grasp of the facts, and a trust in their accuracy, can informed questions be asked and appropriate decisions made.

This first volume is dedicated to the National Security Agency wiretapping controversy. In researching it, we have uncovered a number of fascinating aspects of the public discussion. The very first thing we noticed was the extreme difficulty of establishing the facts. We found, in the press and elsewhere, hunches and guesses, accusations and disclaimers, and a general lack of solid information. For example, experts and policymakers alike disagree on whether or not there has been surveillance, intentional or otherwise, of domestic-to-domestic calls. The debate therefore has concerned not just the legal and political merits of the program, but the details of the program itself. While significant portions of the administration's legal analysis underlying the NSA program have been released (such as the Department of Justice report cited herein), other internal legal and policy documents, if they exist, are not in the public domain. Still, we have persisted in our research. We have enhanced our study of congressional testimonies, press reports and the statements of government officials by consulting experts, policymakers, and administration officials.

We found in our analysis that one topic continually rose to the surface – that of presidential powers. The questions are:

- How far do the president's powers extend in the realm of national security?
- Does the president have the authority, when national security is at stake, to act outside the parameters of a congressionally passed statute?
- Is a statute unconstitutional if it restricts the president's ability to protect the country?

Further questions were subsets of the executive power debate. They included questions about the need for secrecy as a means of ensuring national security, about the evident gap in oversight and accountability, about the sufficiency of existing laws to adapt to changing technology and circumstances, and about the "express will of Congress" as discussed in the classic presidential powers concurrence written by Justice Jackson in the 1952 *Steel Seizures* case.

The debate over the NSA program involves the very questions and considerations that are central to most of the policy debates in the area of law and security in the post-9/11 era. In the matter of NSA wiretapping – as in so much else since 9/11 – the policy issues have concerned whether or not the war on terror requires a paradigmatic shift in understanding the balance of powers and other constitutional issues. Like the matters of detention for enemy combatants, the necessity of secrecy, the role of Congress, the right to habeas corpus, and the validity of coercive interrogation and of pre-emptive justice, the debate over warrantless electronic surveillance is one that requires Americans, both citizens and lawmakers alike, to think carefully about the need for fundamental change and to consider thoughtfully, and outside of political strategies, the tension between customary procedures of established law and emergency exceptions to them. *For the Record* is an attempt to help readers make these decisions for themselves in an informed and balanced way.

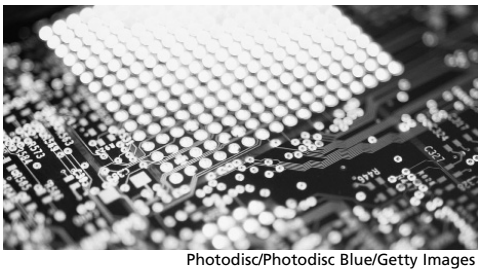
– Karen J. Greenberg

"Attorney General Gonzales, when Members of Congress heard about your contention that the resolution authorizing the use of force amended the Foreign Intelligence Surveillance Act, there was general shock ....

* * *

Now, my reading of this situation legally is that there has been an express statement of Congress to the contrary and if the President seeks to rely on his own inherent power, then he is disregarding congressional constitutional power."

Senator Arlen Specter, (R-Pa.), Chair of the Senate Judiciary Committee, February 6, 2006



Photodisc/Photodisc Blue/Getty Images

What We Know About the NSA Program

The NSA surveillance program began immediately after 9/11, and it was formally authorized by President Bush in October, 2001. The NSA previously required a warrant from the Foreign Intelligence Surveillance Court to conduct electronic surveillance on any domestic phone calls, even if one end was overseas. The new program allows the NSA to conduct warrantless surveillance on international calls with one of the parties inside the United States.[1]

Some phones and individuals are specifically targeted due to their suspected connections to al Qaeda or affiliated groups. These types of intercepts we refer to in this document as "targeted surveillance." In these cases, the NSA has some information that has drawn their attention to these people or phones.[2]

Additionally, the NSA conducts "trawling surveillance."[3] This program appears to conduct electronic screening of a wider range of data or calls and by using electronic search technologies for key words, names or numbers (perhaps to include voice recognition). From that process, more targeted action is taken against suspected individuals or telephones.[4]

The new NSA program raises several legal and policy issues:

- In authorizing this program, has President Bush violated the law?
- Whatever the law may currently say, should the law require the federal government to get a warrant for any call that is surveilled if one of the parties is in the United States (assuming the government has some knowledge of this target)?
- Is the federal government authorized, without a warrant, to conduct electronic trawling surveillance – to sift through broader swaths of calls for words or data – if one of the parties is in the United States?
- What is the role of the Congress (especially select leaders and intelligence committees) in providing oversight of these programs?

The Fourth Amendment of the U.S. Constitution affirms

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[5]

Background

1967 *Katz v. United States*:[6]

The Supreme Court ruled that Fourth Amendment protections extend to electronic surveillance of phone conversations.

1968 Title III of the Omnibus Crime Control and Safe Streets Act:[7]

- Enacted in response to *Katz*.
- For the first time, law enforcement officials were mandated to obtain search warrants to conduct electronic surveillance of phone conversations (known as "Title III" warrants, normally for criminal investigations).
- Title III established procedures to enable judges, after issuing warrants, to exercise continuing oversight and control over the scope of surveillance.
- Title III did not add to any existing limits on the president's surveillance power while acting in the national security sphere: "Nothing contained in this chapter … shall limit the constitutional power of the president to take such measures as he deems necessary."

1972 The *Keith* Case:[8]

- This case addressed warrantless electronic surveillance of *domestic* organizations believed to be attempting to attack the government.
- The government argued that the president could conduct such warrantless surveillance under the national security exemption in Title III.
- The Court found that the domestic security concerns presented in the case did not justify departing from traditional Fourth Amendment requirements, but noted that the facts did not present the question of the scope of the president's authority to conduct warrantless surveillance with respect to the activities of foreign powers.
- The Court reiterated that the holding did not apply to surveillance of foreign powers and their agents, noted that Title III procedures might not be applicable even to domestic threats to national security, and suggested that Congress might write an alternate statute providing protections appropriate to this type of domestic surveillance.

1978 The Foreign Intelligence and Surveillance Act (FISA):[9]

- FISA requires the executive branch to get a warrant to conduct "electronic surveillance" in investigations linked to national security, but the standard differs from that for criminal warrants.
- "Electronic surveillance" is defined in FISA to include any monitoring of "wire communications" that involve a party in the U.S.
- FISA deletes the national security exemption of Title III. It provides that Title III and FISA are "the exclusive means by which electronic surveillance … may be conducted."

FISA Warrants

Normally government agencies investigating criminal cases obtain a "Title III warrant" in which "probable cause of criminal activity" must be shown, as well as "probable cause" that the instrument to be surveilled will be used in that criminal activity. In terrorism or other national security cases involving an individual on U.S. soil, government agencies can instead obtain a "FISA warrant," which requires a lower level of proof and less oversight.

FISA warrants require "probable cause" to suspect that an individual is acting either for a "foreign power" (including terrorist organizations) or as an "agent of a foreign power," a target (a cell phone, a computer, a BlackBerry, or a landline phone, for example), and that foreign intelligence be a "significant purpose" of the warrant.

Under FISA, it is more difficult to assert that a U.S. person (a citizen or permanent resident) is an agent of a foreign power than a non-U.S. person. For U.S. persons, there must be probable cause that their activity may involve the commission of a national security crime.

Surveillance on targets located outside U.S. territory is not limited by Fourth Amendment protections and has traditionally been left to the complete authority of the executive branch. Domestic targets, however, do have Fourth Amendment protection, leading to the Title III and FISA restrictions on government activity.

Applying for a FISA Warrant

A FISA application must include the following:

- Information to justify the belief (i.e. supply the "probable cause") that the target is an agent of a foreign power and that the electronic devices are used by the target.
- A detailed description of the information sought and the type of communications to be subjected to surveillance.
- A certification and basis for the certification by an executive branch official that the information sought is foreign intelligence information, that a significant purpose of the surveillance is to obtain foreign intelligence information, and that such information cannot be reasonably obtained by normal investigative techniques.
- The means of surveillance, and whether physical entry will be required.
- The period of time required.

"This is not a backdoor approach. We believe that Congress has authorized this kind of surveillance." Attorney General Alberto R. Gonzales, December 19, 2005

The Foreign Intelligence Surveillance Court

FISA warrants are adjudicated by the Foreign Intelligence Surveillance Court, in classified, closed sessions at the Justice Department in Washington.[10] The court consists of eleven federal judges, selected by the Chief Justice of United States, who review FISA warrant applications. Each judge is appointed to a seven-year term. The order can authorize surveillance for 120 days or the duration necessary, whichever is less. After this period an application for an extension can be filed. The maximum extension is for one year.

Emergency Surveillance Without a Warrant

A FISA judge is always on call. However, FISA also contains three provisions for emergency surveillance without a warrant.

1) In the event of a congressional declaration of war, FISA allows warrentless surveillance "for a period not to exceed fifteen calendar days," after which the president would be expected to either resume FISA compliance or seek new legislation tailored to the circumstances.

2) FISA allows the attorney general, without seeking judicial approval, to order surveillance of foreign government entities for periods up to a year. This authority doesn't apply to surveillance of international terrorist groups that aren't governmental entities. It is only available when "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."

3) FISA allows surveillance of any foreign agent (including U.S. persons) on an emergency basis for periods not to exceed 72 hours. Under this authority, the attorney general must "reasonably determine" that "an emergency situation" exists and ascertain the facts of the case.

- The attorney general must inform a FISA judge that emergency electronic surveillance has been initiated.
- A FISA warrant application must be made as soon as is practicable but not more than 72 hours after the attorney general authorizes the surveillance to begin.
- The surveillance must stop as soon as the requisite information is collected, or if the application is denied by the FISA judge. If the application is denied, the target of the surveillance must be notified of the government's activity, and no information collected during the surveillance may be used or disclosed in court unless the attorney general finds that the information indicates a threat of death or serious bodily harm to any person.

2001 PATRIOT Act Amendments to FISA (Relevant to the NSA Program)[11]

- All communication devices of an individual can now be targeted with "roving surveillance." Previously a FISA warrant could only be filed in relation to one device.
- Third parties (e.g. landlords or telecommunications carriers) cooperating in setting up a wiretap do not need to be named in the warrant request.

2004 The "Lone Wolf" Amendment to FISA[12]

The grounds for filing a FISA warrant were expanded to include individuals who are not clearly foreign agents or working for terrorist organizations. The definition of "an agent of a foreign power" was broadened to include any non-U.S. person "who engages in international terrorism or activities in preparation therefore."

	Title III Warrants	FISA Warrants	Emergency FISA *(no warrant required)*
Uses	Domestic criminal cases	Foreign intelligence information cases targeting foreign powers or their agents	For third type, same as standard FISA; no special grounds required for the other two types
Must Show	Probable cause of criminal activity, and probable cause that target device would be used to further it	Probable cause that that suspect is acting for a foreign power or as an agent of a foreign power; for U.S. persons, probable cause of a criminal or national security threat; plus probable cause that device(s) will be used by target of surveillance	For third type, attorney general must attest that information in box to the left is supplied within 72 hours
Wiretapping Can Begin	Only after judicial approval	Only after judicial approval	For the third type, after attorney general approval (but judicial review required within 72 hours)
Judicial Oversight	Warrant expires and law enforcement must reapply after 30 days (or less)	Warrant expires and law enforcement must reapply after 90 days (or less) for surveillance of U.S. persons; 120 days (or less) for others	For third type, same as standard FISA
Congressional Oversight	Annual report must be filed with the federal court system's administrative office	Attorney general must report to the congressional intelligence committees annually, but report requires less detail than Title III annual filing	Included in the attorney general's report
Notice to Individuals	Target of surveillance must be notified of surveillance when warrant expires	Target of surveillance must be notified of surveillance only if the government intends to use the evidence in a proceeding	For third type, same as standard FISA, except target must be notified if application is denied

How the NSA Program Works

The NSA Program

The NSA program began in the immediate wake of 9/11. It allows the NSA to target phone calls without a warrant when one of the callers is outside the United States and the intercept is done on U.S. soil. The program was retroactively authorized by a secret executive order in early October, 2001.[13] The program is reviewed every 45-60 days, and had been renewed over thirty times by the middle of December, 2005.[14]

According to *The New York Times*, the NSA has used the program to eavesdrop without warrant on as many as 500 international calls at any given time since 2002. Separately from the new program, about 5,000 to 7,000 people are being monitored overseas.[15] This targeted surveillance is triggered by suspicious names or phone numbers on intelligence watch lists. A call can be monitored if the NSA shift supervisor has a "reasonable belief" that someone on either end has links to al Qaeda.[16] For purely domestic calls, a FISA warrant requires a higher showing of probable cause that must be identified in the written request for authorization.

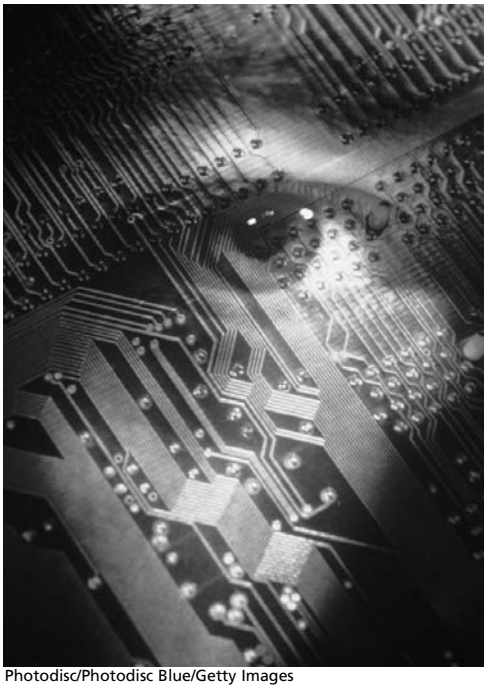
Two Types of Surveillance: Trawling and Targeted

We define "trawling surveillance" as NSA interception of entire streams of communications, which are then subjected to computer analysis for particular names, internet addresses, and trigger words. "Targeted surveillance" refers to intercepts focused on one person or phone number. The NSA has authorization to use both sorts of surveillance on purely overseas calls without a warrant, and it does. The agency is not authorized to conduct either sort of surveillance on purely domestic calls. It's not clear, however, whether the new program authorizes trawling surveillance on a stream of calls in which one side of the conversation is overseas, and the intercept is made on U.S. soil. According to several credible news sources, this type of surveillance did in fact take place under the new program.[17]

The New York Times reports that accounts from administration officials have been contradictory, but that some say "purely domestic communications have been captured because of the technical difficulties of determining where a phone call or e-mail message originated."[18] For inadvertently collected domestic calls, the NSA "minimizes" the data. In other words, all records are deleted unless analysis indicates the call is of a criminal or national security concern. If so, the NSA alerts the Justice Department under strict guidelines that limit dissemination and action on the information.[19]

In discussing the legal and management aspects of these programs, both targeted and trawling surveillance must be considered. On November 27, 2006, the inspector general of the Justice Department said that his office would review the department's use of information from the NSA program.

"This is a different era, a different war [and] we've got to be able to detect and prevent. I keep saying this but this … requires quick action." President George W. Bush, December 19, 2005



Photodisc/Photodisc Blue/Getty Images

The Congressional Role

Congressional Oversight of Intelligence Activities[20]

The National Security Act of 1947 regulates congressional oversight of U.S. intelligence activities. The president is to ensure that the congressional intelligence committees are kept "fully and currently" informed of U.S. intelligence activities, including "significant anticipated intelligence activity."[21]

Briefing Congress

President Bush has stated that executive branch representatives briefed congressional leaders more than a dozen times on the NSA program.[22] However, some members of Congress who were briefed on the program said the briefings had been limited to the Gang of Eight (the majority and minority leaders of both houses and the chairmen and ranking members of both intelligence committees). That group traditionally oversees covert actions,[23] but only in "extraordinary circumstances affecting vital interests of the United States."[24]

At least one member of the group found this limitation inappropriate, since the NSA program (according to her assertion) could not qualify as a covert action.[25]

The Gang of Eight was first told of the nature and scope of the NSA program in early October, 2001.[26] Two group members who were briefed said that they voiced concerns over the program but were not given an opportunity to either approve or disapprove.[27] Others said that they could not recall these objections.[28] Some members also asserted that the executive branch had prohibited them from sharing information about the program with congressional colleagues, including members of the two congressional intelligence committees.[29]

Staff members were also barred from these briefings. Members of the Gang of Eight have asserted that, without being able to consult staff, it was impossible to effectively question the administration on the program.[30]

Two senators, John D. Rockefeller (D-W.Va.) and Nancy Pelosi (D-Calif.), have stated that they sent letters to Vice President Dick Cheney expressing concerns about the program after they were briefed and that their concerns were not addressed. They have not disclosed the content of those letters.[31]

Congressional Bills to Amend FISA

On September 13, 2006, the Senate Judiciary Committee approved three bills to be referred to the full Senate amending FISA. These were:

Specter-Feinstein Bill[32]

Submitted May 24, 2006, the bill would retain FISA as the exclusive means to conduct electronic surveillance of foreign powers and agents of foreign powers.

Specter Bill[33]

Submitted July 13, 2006, the bill was put forward after negotiations with the Bush administration. The bill states that FISA is not intended to limit the constitutional authority of the president to conduct electronic surveillance of foreign powers and agents of foreign powers.

DeWine Bill[34]

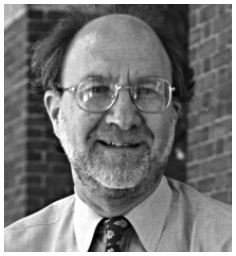
Submitted March 16, 2006, by Senators Mike DeWine (R-Ohio), Lindsey Graham (R-S.C.), and Chuck Hagel (R-Neb.), the bill would allow the president to conduct electronic surveillance without warrant for renewable periods of 45 days.

On September 28, 2006, the House of Representatives approved a bill by Heather Wilson (R-N.M.), which would allow the president to conduct electronic surveillance without warrant for renewable periods of 45 days after a terrorist attack.[35] The House and Senate to date have failed to come to an agreement on legislation to amend FISA.

Ask the Experts: The Debate Over the NSA Program


Bryan Cunningham


Mary DeRosa


Stephen Schulhofer

Our *For the Record* series is intended to present the facts underlying topics that are often politically charged. In "Ask the Experts," a feature to be included in each volume, we will present diverse viewpoints from attorneys, policymakers and scholars who grapple with these issues every day, in order to show the scope of professional debate. In this inaugural volume, **Bryan Cunningham**, **Mary DeRosa**, and **Stephen Schulhofer** address the ability of FISA to handle ever-evolving terrorist threats, and the need for the NSA's wiretapping program.

Bryan Cunningham is an information security and privacy lawyer at the Denver law firm of Morgan & Cunningham LLC. Previously, Mr. Cunningham served six years in the Clinton administration in senior CIA positions and as a federal prosecutor, and, for two years, as deputy legal advisor to National Security Advisor Condoleezza Rice, where he drafted portions of the Homeland Security Act and was involved in the formation of the National Strategy to Secure Cyberspace. Along with the Washington Legal Foundation, he has filed "friend of the court" briefs in support of the NSA program in United States District Court and the Court of Appeals.

Mary DeRosa is a senior fellow at the Technology and Public Policy Program of the Center for Strategic and International Studies (CSIS). She joined CSIS in this position in 2002, after serving as special assistant to the president and legal adviser on the National Security Council staff during the Clinton administration. Previously, she was a lawyer at the Department of Defense and in private practice at the firm of Arnold & Porter.

Stephen Schulhofer is the Robert B. McKay Professor of Law at the New York University School of Law. He is the author of more than 50 scholarly articles and six books, including *The Enemy Within: Intelligence Gathering, Law Enforcement* and *Civil Liberties in the Wake of September 11* (2002) and most recently, *Rethinking the Patriot Act* (2005), both written for The Century Foundation's Project on Homeland Security. He completed his B.A. at Princeton and his J.D. at Harvard, both summa cum laude. He clerked for two years for U.S. Supreme Court Justice Hugo Black, and has served as the Ferdinand Wakefield Hubbell Professor of Law at the University of Pennsylvania and the Julius Kreeger Professor of Law and director for Studies in Criminal Justice at the University of Chicago.

Is FISA Too Cumbersome? Too Slow?

Supporters of the NSA program:
The administration has stated that the FISA warrant procedure is too cumbersome and slow. Attorney General Alberto Gonzales has said, "it still takes too long to get FISAs approved. FISA applications are often an inch thick and it requires a sign off by analysts out at NSA, lawyers of the department and finally by me. And then it has to be approved by the FISA court."[36] Proponents of the program have said that even the emergency warrant process may be too slow.

Bryan Cunningham and colleagues, for example, said in a recent court filing:

> As a practical matter, in many hypothetical situations, this requirement to demonstrate all of the substantive and procedural elements of FISA to the Attorney General's satisfaction before *any surveillance can begin*, would fatally impair the President's ability to carry out his constitutional responsibility to collect foreign intelligence to protect our Nation from attack.
>
> Assume, for example, the United States Government is conducting electronic surveillance, pursuant to a FISA order, on a telephone call from Osama bin Laden to a U.S. person, John Doe, inside the United States. Assume further that the government hears bin Laden informing John Doe that a chemical, biological, or nuclear device hidden in a U.S. city is armed, and that the device will be detonated by another U.S. person in the United States, David Roe, upon receiving instructions two minutes later from a previously unknown al Qaeda operative outside the United States who will then disclose the location and

detonation method for the weapon.

Obviously, under even the most favorable conditions, it would be literally impossible to gather and present to the Attorney General the required information to meet all of FISA's procedural and substantive requirements, within two minutes, in order to intercept the upcoming international call from the al Qaeda operative to David Roe, including those FISA elements that must be demonstrated by probable cause, in order to invoke FISA's "emergency" authority to begin conducting the surveillance.[37]

Critics of the NSA program:

Critics of the NSA program do not necessarily object to the type of surveillance, but rather to the way in which it has been authorized, and to the absence of any oversight. They argue that the NSA has recourse to the emergency warrant procedure to speed applications. In addition, they say that the answer to problems with the efficiency of the FISA application process should be to solve those problems. Finally, they say that most problems with the speed of the FISA application process are due to the executive branch's own policies and procedures, rather than FISA itself.

Mary DeRosa agrees that the FISA process is cumbersome, but said that "this is a problem not with the law, but with the bureaucracy."[38] She also said that:

> The most consistent complaint about FISA from those who must use it is that the administrative requirements for seeking a warrant make the process unduly difficult and time-consuming. People speak of burdensome paperwork and significant delays in the Justice Department approval process. Applications can be put on a fast track if they are urgent, but this is an ad hoc and unsatisfactory process. In addition, FISA's emergency provision permits the conduct of surveillance for 72 hours before seeking a warrant, but procedures within the executive branch for exercising this option are also burdensome. In any event, it is bad governance at best if the government must invoke an emergency procedure because its own bureaucracy is too stifling.[39]

But **Ms. DeRosa** believes that the answer is for the executive branch or Congress to fix these bureaucratic problems. "It is not clear," she said, "that these bureaucratic problems are due to the language of FISA itself; many can be attributed to executive branch procedures that have developed over time. The executive branch has the responsibility to improve its own procedures if it finds them to be an impediment to national security. But in this case, where there is plenty of evidence of a problem, Congress can and should act to improve the situation."[40]

Opponents of the NSA program:

FISA already provides, **Stephen Schulhofer** said, that electronic surveillance can begin on an emergency basis as soon as the attorney general is satisfied that an emergency exists and there is a factual basis for an order (i.e. target is a foreign agent, and that minimization procedures are followed). "If there is a need to go further," he added, "neither the struggle against terrorism nor the complexities of new technologies can justify conferring on the executive branch surveillance powers that are completely unchecked and unreviewable. Any congressional fix should insure some system of oversight – there are many possibilities that can guarantee accountability and prevent overreaching without jeopardizing legitimate secrecy needs."[41]

Is FISA Outdated?

Supporters of the NSA program:

The Bush administration has argued that new telecommunications technologies have made it impossible to effectively track al Qaeda through the FISA warrant procedure.

Bryan Cunningham said that:

> [T]here are a host of technological developments which have rendered FISA, as currently drafted, unworkable against the post-9/11 terrorist threat 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, and the routing of vast amounts of purely overseas Internet communications through the United States….
>
> Equally fatal to the ability of any president to comply with all of the substantive and procedural requirements of the 1978 FISA is the current statute's target-by-target dependence upon two principal factors for determining the predicates necessary for approval of intercepts: 1) whether or not a potential target is a known or presumed United States person (a citizen or a permanent resident alien); and 2) whether the collection of information takes place within the territory of the United States or overseas …. These two pieces of information often will be unknowable given today's (and tomorrow's) technology – or at least unknowable in a timely enough way to secure FISA warrants to capture brief but crucial terrorist attack warning information.[42]

Critics of the NSA program:

Critics of the NSA program argue that the statutory framework can adjust for evolving communications technology. To the extent that FISA may appear to present obstacles, or where there may be confusion as to what it prohibits, Congress should review and clarify its definitions, they say. To the extent that it may be outdated, it should be amended. However, critics argue, there is no need to abandon the act to the extent of using the NSA program with no oversight or accountability instead.

Mary DeRosa said that:

> FISA is actually more flexible than many people give it credit for. It is certainly not a model of clarity – its language is dense almost to the point of being unreadable …. But those who have interpreted and applied FISA through the years know it has been flexi-

ble enough to adapt to many changes in technology and threat….The FBI has not found itself "paralyzed" in attempting to pursue possible connections to terrorism, as some have suggested.… Clarifying some aspects of the law would be helpful to the Executive Branch in carrying out its responsibilities.

One area of the law that could be clarified, she continued, are the rules for purely international calls that pass through the United States en route to their destination:

> It is my understanding that intercepting this type of communication would not be "electronic surveillance" subject to FISA's provisions because it does not involve targeting a communication to or from at least one person who is located in the United States. If there is confusion about this point that causes the executive branch difficulty in carrying out its surveillance activities, the legislation should be clarified.…
>
> FISA is adequate to the current task of electronic surveillance, but it almost certainly is not optimal. A careful review by Congress of FISA's definitions and requirements, informed by administration input, could result in useful changes to make FISA even more adaptable.[43]

She also said that "It would be good if FISA could get an honest overhaul."[44]

While FISA's critics argue that the statue's language is too tangled to be of practical use, **Ms. DeRosa** counters that the NSA program provides little effective guidance of its own. "What can't they do?" she asked, "Where's the clarity there?"[45]

Opponents of the NSA program:

Even if FISA requirements are no longer suited to law enforcement and counterterrorism needs, those requirements must be updated by Congress rather than through an executive order, opponents say.

Stephen Schulhofer said that:

> [T]he NSA program is a scandal not only because of the program's impact on privacy, but more importantly because the program represents a direct assault on our constitutional structure and its commitment to the separation of powers. The Framers of our Constitution deliberately chose not to give the President the power to rule by decree, even under emergency circumstances. Precisely because reasonable people can disagree about the kind of electronic surveillance that should be permissible and the kind of oversight safeguards that are necessary, the judgment about whether and how to change the law must be made through democratic deliberation in Congress, as our Constitution contemplates. It should not be made by unilateral decisions taken in secret by the President and his inner circle of advisors. Even if one knew exactly what the NSA program entails (none of us in the general public does), and even if one thought its details were all perfectly appropriate, the program's most dangerous feature would remain – its claim that because we are "at war," the president can unilaterally change the laws and disregard the laws at will.[46]

Does FISA Unconstitutionally Limit the President's Inherent Powers?

Supporters of the NSA program:

The administration and proponents of the NSA program have made the argument that it is supported by the president's inherent constitutional authority.[51] According to this argument, foreign policy and foreign intelligence are areas specifically and constitutionally left to the authority of the president, in accordance with the separation of powers.[52] This encompasses a power to conduct warrantless searches for foreign intelligence purposes.[53] If this is correct, any aspect of FISA which undermines this inherent authority would be unconstitutional. This argument is supported by a Fourth Circuit case decided in 1980,[54] as well as one recent decision by the Foreign Intelligence Court of Review,[55] but the issue has never been directly decided by any Supreme Court case.[56]

The administration has also argued that FISA allows electronic surveillance authorized by other statutes, and that the Authorization to Use Military Force qualifies as a statute authorizing electronic surveillance.

Critics of the NSA program:

Critics of the program argue that FISA limits the president's authority to conduct warrantless wiretaps and explicitly sets forth the "exclusive means" by which the president may conduct electronic surveillance for national security within the United States. The AUMF cannot be read to trump the clear and specific language of FISA, they say.[57] Had Congress intended to amend the statute in so fundamental a way, they argue, Congress would have actually amended it.[58] One Supreme Court case supports this interpretation, stating that statutes may only be repealed when there is "overwhelming evidence" that Congress intended to do so.[59]

Moreover, critics argue that the president does not have the inherent authority he claims.[60] They note that "[e]very time the Supreme Court has confronted a statute limiting the Commander-in-Chief's authority, it has upheld the statute,"[61] and argue that even very recently the Court unanimously refused to accept the argument that the president could not be limited by congressional oversight when acting as commander in chief.[62] They also argue that the cases relied upon by the administration dealt with pre-FISA circumstances, and never directly addressed the question of whether FISA could constitutionally limit the president's powers in these areas.[63] Finally, they argue that Fourth Amendment case law does not allow for this type of surveillance.[64]

Opponents of the NSA program:

Opponents say that the president has no legal authority to authorize the NSA program, either through his inherent constitutional powers or through the AUMF.

Stephen Schulhofer said that:

> [T]he NSA program is unquestionably illegal. FISA states explicitly that compliance with its procedures or those of

Title III is the "exclusive" means by which electronic surveillance may be conducted. The administration has argued that the vague language of the AUMF, a resolution enacted a week after 9/11, overrides statutory restrictions that were in force before 9/11. But this strained argument was expressly rejected by the Supreme Court in *Hamdan v. Rumsfeld*, where the Court held that "there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter" pre-existing statutory restrictions.[65] It was reasonably clear before *Hamdan*, and is now clear beyond any possible doubt, that the NSA program violates existing law. The violation, moreover, was inexcusable. FISA has been amended many times since 9/11. The Administration could have sought Congressional approval for any further legal changes justified by the circumstances.[66]

With respect to the argument that FISA's restrictions might be unconstitutional, **Prof. Schulhofer** added that:

> [A]lthough the Constitution designates the President as "commander in chief," thus assuring that military forces will be controlled by civilian authority, the Constitution does not give the President sole responsibility for managing military affairs. To the contrary, Article I, section 8, gives explicitly to Congress, not to the President, the power to "make Rules for the Government and Regulation of the land and naval Forces." Thus, even if electronic surveillance is considered a tool of military operations, the Constitution expressly and unambiguously gives Congress the power to regulate its use. The Administration's attempt to argue otherwise is not merely incorrect; it is frivolous and disingenuous.

The *Steel Seizures* Case and the Authorization to Use Military Force

In 1952, during the Korean War, a breakdown in negotiations between the Youngstown Sheet & Tube Company (a steel mill) and its workers led the steelworkers' union to give notice of a nationwide strike. Due to the repercussions that a strike would have had for the war effort, President Harry Truman issued an executive order directing the secretary of commerce to take possession of U.S. steel mills. Mill owners complied, but soon claimed that the order constituted an unlawful seizure. President Truman responded that his actions were supported by his inherent presidential powers under the Constitution, due to the threat a strike would have posed to the war effort.

Justice Hugo L. Black gave the opinion of the Court, finding that President Truman had overstepped his bounds, and that his authority as commander in chief did not include a power to seize property needed for the war effort, in the absence of congressional action granting such power. Justice Robert H. Jackson's often-cited concurrence provides a framework to analyze the extent of presidential powers in any given situation. He stated:

- "There is a zone of twilight in which [the president] and Congress may have concurrent authority, or in which [the distribution of power between the two] is uncertain."[47]
- Therefore, "When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."[48]
- When Congress has neither granted nor denied the power involved, Justice Jackson stated the determination of constitutionality will be more fact-based, and particular to the circumstances.
- "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."[49]

FISA is an express congressional denial of power, as it revoked the national security exemption of Title III and states that FISA and Title III will be the exclusive means to conduct electronic surveillance. However, the Authorization to Use Military Force (AUMF), a resolution enacted a week after 9/11, grants the president the authority "to use all necessary and appropriate force against those nations, organizations or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism."[50] The administration has argued that the AUMF constitutes implied authorization to conduct surveillance not permitted by FISA. Critics argue that the AUMF was intended to authorize the deployment of military force in its conventional sense and was not intended to give the president a blank check to ignore laws that apply to specific governmental actions within the United States.

Interview with Michael Sheehan (Distinguished Senior Fellow)

Is FISA appropriate now?

FISA was passed in 1978, and although modified somewhat, it is still in the Stone Age. The threat environment has changed, terrorists have struck us at home and the revolution in the global telecommunications industry has been enormous. The old laws are as outdated as an old switchboard operator.

How would you amend FISA?

Number one, FISA needs to be streamlined. My experience in New York City was that it was too slow – it took months to get a FISA passed through the system – and people were reluctant to go to an emergency FISA except under very specific circumstances. For the non-emergency FISA, I thought the time lag was unacceptable. The problem was not the FISA court but the endless editing and re-editing of documents by lawyers and bureaucrats in both the FBI and DOJ.

Secondly, FISA needs to be updated to cover the electronic surveillance program initiated by the Bush administration in the wake of 9/11. Good SIGINT (signals intelligence) is a critical component in the counter terrorism business and we need good legislation for these programs.

Is the president right?

I think the president was right to tap those calls after 9/11. Nineteen terrorists operating in our country had just killed almost 3,000 of our fellow citizens. The NSA had an obligation to see if other international communications with al Qaeda operatives was taking place to or from the United States. And in fact they were; some of it right here in New York City.

But the critics were also right in identifying that the law should be updated to meet the new threat and the technological challenges of the program. The president should have sought more explicit authority – and I think he would have gotten it.

We need a program and laws that enable the NSA to be aggressive, and we need safeguards that protect American citizens from intrusions on their privacy. I think that balance can be reached.

What about congressional oversight?

I think the Congress must be much more aggressive in demanding that its constitutional duties of oversight are implemented. Of course, that is sometimes difficult when you have one party controlling both the executive and congressional branches. In this case, the Republican members were expected to tow the line. And the Democrats seemed to defer for security or other reasons. Both sides should have put their objections in writing to the president (not to Vice President Cheney, as done by some Members), and with copies to the relevant agency heads. In government, if you don't write and properly disseminate it, the objection does not really exist.

Both sides of the aisle have a duty to step up and get into the game much more aggressively. They have the ultimate leverage over the administration, the power of the budget. And they need to play hardball, as necessary, to make sure the appropriate members of the administration are up on the Hill briefing members in detail as to what the administration is doing.

It is my experience that if you consult with congress in good faith you can get a lot of cooperation, and they generally do not leak. That comes from the executive branch mostly, and from both parties, and I have worked in both Democratic and Republican administrations. If people leak, they should be prosecuted, even if it is your chief of staff.

Is a complete overhaul needed?

Yes.

The NSA and Electronic Surveillance

CREATION:
The NSA was created pursuant to a memorandum issued by President Truman in 1952, replacing the Armed Forces Security Agency.

LEADERSHIP:
The current director of the NSA is Army Gen. Keith B. Alexander. By law, all NSA directors must be commissioned military officers.

PRIMARY RESPONSIBILITIES:
Signals intelligence (exploitation of foreign communications) and information assurance (protection of U.S. information systems).

CONGRESSIONAL OVERSIGHT:
The NSA is overseen by the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Defense Subcommittee of the Senate Appropriations Committee, and the Defense Subcommittee of the House Appropriations Committee.
For covert operations, eight members of Congress are briefed by NSA. They are known as the "Gang of Eight."

Chronology

- Immediate wake of 9/11 – Surveillance program initiated.
- October, 2001 – The administration informs the "Gang of Eight." In the same month, the program is authorized by secret executive order.
- April, 2002 – The administration tells Royce C. Lamberth, presiding judge of the FISA court, about the program.[67]
- Mid-2004 – Judge Colleen Kollar-Kotelly, presiding over the FISA court, expresses concerns about the program, leading to a Justice Department audit. At this time, the administration changes aspects of the program, but details are unavailable.[68]
- 2004 - Congressional leaders tell the administration that trying to amend FISA to explicitly authorize the program would inevitably undermine it, according to Attorney General Alberto Gonzales's congressional testimony on February 6, 2006.
- January 17, 2006 – The American Civil Liberties Union files a complaint in federal court in Michigan, alleging that conversations of individuals in the U.S. are being improperly monitored through targeted surveillance and automated data-mining (trawling).
- February, 2006 – The Senate and House Intelligence and Judiciary Committees start a series of hearings on the program.
- July 13, 2006 – Senator Arlen Specter (R-Pa.), chair of the Senate Judiciary Committee, introduces a bill proposing amendments to FISA legislation. This plan is the product of weeks of negotiation between the White House and Senator Specter. One of the bill's provisions, consented to by President Bush, would give the FISA court jurisdiction to rule on the program's constitutionality.
- July 14, 2006 – Representative Heather Wilson (R-N.M.) proposes legislation in the House to amend FISA.
- August 17, 2006 – Judge Anna Diggs Taylor of the U.S. District Court for the Eastern District of Michigan, ruling in the ACLU case, finds the targeted surveillance portion of the NSA's program unconstitutional. However, she dismisses the data-mining claim because it could not be litigated without revealing state secrets. Judge Taylor temporarily stays her order to end the program until it can be considered by the appellate court.
- September 13, 2006 – The Senate Judiciary Committee approves three bills that would amend FISA (the Specter bill, the Specter-Feinstein Bill, the DeWine Bill).
- September 25, 2006 – Senator Specter agrees to three amendments to his bill, but it has not been put in front of the full Senate.
- September 28, 2006 – The House approves the Wilson bill, making it unlikely that Senate and House Republicans would amend FISA before the November 2006 midterm elections.
- October 4, 2006 – The United States Court of Appeals for the Sixth Circuit allows the program to continue while it considers the administration's appeal in the ACLU case.
- November 27, 2006 – The inspector general of the Justice Department says that his office will review the department's use of information from the NSA program.

Sources

OUTLINING THE PROGRAM

Interview with Kevin O'Connell, former NSA official, in New York, N.Y. (Sept. 30, 2006).

Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Comm. on the Judiciary, 109th Cong. (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States).

Alberto Gonzales, Att'y Gen. of the United States, & General Michael Hayden, former head of the Nat'l. Sec. Agency & Deputy Dir. of Nat'l Intelligence, now Dir. of the CIA, Press Briefing at the White House (December 19, 2005) (transcript available at http://www.white-house.gov/news/releases/2005/12/20051219-1.html).

General Michael Hayden, former head of the Nat'l. Sec. Agency & Deputy Dir. of Nat'l Intelligence, now Dir. of the CIA, News Conference at the National Press Club (January 23, 2006) (transcript available at http://www.democracynow.org/article.pl?sid=06/01/24/1516258#transcript).

James Risen, State of War (2005).

Ron Suskind, The One Percent Doctrine (2006).

James Bamford, *Big Brother is Listening,* The Atlantic, April 2006, at 65.

National Security Law Report (A.B.A. Standing Committee on Law and National Security), March 2006.

N.Y.U. Rev. L. & Sec., No. VII: *The NSA and the War on Terror* (Supp. Spring 2006).

James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, December 16, 2005, at A1.

LEGAL DIMENSIONS

U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (*Justice Dep't. White Paper of Jan. 19*) (2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf.

Brief for Washington Legal Foundation as Amicus Curiae in Opposition to Plaintiffs' Motion for Partial Summary Judgment and in Support of Defendants' Motion to Dismiss, or in the Alternative, for Summary Judgment, Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (No. 06-10204).

Memorandum from Alfred Cumming, Specialist in Intelligence & Nat'l Sec., Cong. Research Serv., Statutory Procedures Under Which Congress Is to Be Informed of U.S. Intelligence Activities, Including Covert Actions (Jan. 18, 2006).

Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department White Paper of January 19, 2006 (February 2, 2006).

Stephen J. Schulhofer, The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11 (2002).

Stephen J. Schulhofer, Rethinking The Patriot Act: Keeping America Safe and Free (2005).

David Cole and Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 IND. L.J. 1355 (2006).

Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 Stanford Law & Policy Review 531 (2006).

Balkinization (blog of Jack M. Balkin, Professor of Law, Yale Law School), http://balkin.blogspot.com.

OrinKerr.com (blog of Orin S. Kerr, Professor of Law, Princeton University), www.orinkerr.com.

TECHNICAL DIMENSIONS

Foreign Intelligence Surveillance Act Reform: Hearing Before the H. Permanent Select Comm. On Intelligence, 109th Cong. (July 19, 2006).

Mary DeRosa, Cent. for Strategic & Int'l Studies, Data Mining and Data Analysis for Counterterrorism (2004).

K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance,* N.Y.U. Rev. L. & Sec., No. VII: *The NSA and the War on Terror* (Supp. Spring 2006).

Notes

[1] *See infra* notes 13-14 and accompanying text.
[2] *See infra* note 15-16 and accompanying text.
[3] *See infra* Part 2.
[4] Interview with Kevin O'Connell, former NSA official, in New York, NY (Sept. 30, 2006).
[5] U.S. Const. amend. IV.
[6] 389 U.S. 347 (1967).
[7] Pub. L. No. 90-351, 82 Stat. 212 (1968).
[8] United States v. U. S. Dist. Court, 407 U.S. 297 (1972).
[9] 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-1863 (2000).
[10] James Bamford, *Big Brother is Listening*, The Atlantic, April 2006, at 65.
[11] See N.Y.U. Rev. L. & Sec., No. VII: *The NSA and the War on Terror* (Supp. Spring 2006).
[12] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 2742 (2004).
[13] Ron Suskind, The One Percent Doctrine 37 (2006).
[14] Sheryl Gay Stolberg and Eric Lichtblau, *Senators Thwart Bush Bid to Renew Law on Terrorism*, N.Y. Times, December 17, 2005, at A1. *See also Bush Says He Signed NSA Wiretap Order*, December 17, 2005, http://www.cnn.com/2005/Politics/12/17/bush.nsa/index.html.
[15] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, December 16, 2005, at A1.
[16] Bamford, *supra* note 10, *confirmed by* General Michael Hayden, former head of the Nat'l. Sec. Agency & Deputy Dir. of Nat'l Intelligence, now Dir. of the CIA, News Conference at the National Press Club (January 23, 2006) (transcript available at http://www.democracynow.org/article.pl?sid=06/01/24/1516258#transcript).
[17] James Risen, State of War 51 (2006); Bamford, *supra* note 10.
[18] Scott Shane, *At Security Agency, News of Surveillance Program Gives Reassurances a Hollow Ring*, N.Y. Times, December 22, 2005, at A22.
[19] Interview with Kevin O'Connell, former NSA official, in New York, NY (Sept. 30, 2006).
[20] *See generally* Memorandum from Alfred Cumming, Specialist in Intelligence & Nat'l Sec., Cong. Research Serv., Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions (Jan. 18, 2006) [hereinafter CRS Memo].
[21] Pub. L. No. 80-253, 501-03, 61 Stat. 495 (1947) *as amended by* Fiscal Year 1991 Intelligence Authorization Act, Pub. L. No. 102-88 (current version at 50 U.S.C. §§413-13(a)-(b) (2000)).
[22] Radio Address, President George W. Bush, Dec. 17, 2005, and Town Hall Meeting, President George W. Bush, January 11, 2006 *cited in* CRS Memo, *supra* note 20, at 7.
[23] CRS Memo, *supra* note 20, at 7 (citing Letter from U.S. Representative Jane Harman to President George W. Bush (January 4, 2006), *available at* http://www.house.gov/harman/press/releases/2006/0104PR_nsaprogram.html).
[24] 50 U.S.C. §413b(c)(2) (2000).
[25] Letter from U.S. Representative Jane Harman to President George W. Bush (January 4, 2006), *available at* http://www.house.gov/harman/press/releases/2006/0104PR_nsaprogram.html.
[26] Suskind, *supra* note 13, at 37.
[27] CRS Memo, *supra* note 20, at 7 (citing Press Release, Senator John D. Rockefeller, Vice Chairman Rockefeller Reacts to Reports of NSA Intercept Program in the United States, (December 19, 2005); Nancy Pelosi, *The Gap in Intelligence Oversight*, Washington Post, January 15, 2006, at B7; Press Release, Representative Nancy Pelosi, Pelosi Requests Declassification of Her Letter on NSA Activities (December 20, 2005)).
[28] *Id.* (citing Press Statement, Senator Pat Roberts, Senator Roberts' Response to Media Reports About Senator Rockefeller's 2003 Letter (December 20, 2005); Press Conference, Representative Peter Hoekstra, The Presidential National Security Agency Authorization for Surveillance Without Warrant (December 21, 2005)).
[29] *Id.* (citing Press Release, Senator John D. Rockefeller, Vice Chairman Rockefeller Reacts to Reports of NSA Intercept Program in the United States (December 19, 2005)).
[30] Suskind, *supra* note 13, at 37; *see also* John Diamond, *Congressional Oversight of Intelligence Never Easy*, USA Today, December 20, 2005, *available at* http://www.usatoday.com/news/washington/2005-12-20-intel-oversight_x.htm?csp=1; *NewsHour with Jim Lehrer: Overseeing Surveillance* (interview of Representative Jane Harman) (PBS television broadcast February 8, 2006), available at http://www.pbs.org/newshour/bb/congress/jan-june06/nsa_02-08.html.
[31] Carol D. Leonnig and Dafna Linzer, *Spy Court Judge Quits in Protest: Jurist Concerned Bush Order Tainted Work of Secret Panel*, Washington Post, December 21, 2005, at A1 (Senator Rockefeller saying that he was first briefed on the program in July, 2003 and that he sent a letter shortly thereafter).
[32] Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S. 3001, 109th Cong. (2006).
[33] National Security Surveillance Act of 2006, S. 2453, 109th Cong. (2006).
[34] Terrorist Surveillance Act of 2006, S. 3874, 109th Cong. (2006).
[35] Electronic Surveillance Modernization Act, H.R. 5825, 109th Cong. (2006).
[36] *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Comm. on the Judiciary,* 109th Cong. (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States). Lt. Gen. Keith B. Alexander, head of the NSA, told the Senate Judiciary Committee on July 26, 2006 that it would be "tremendous burden" for the NSA if it had to get a warrant every time a foreign target with suspected ties to al Qaeda communicated with someone who might be in the United States. He added, "You would be so far behind the target, if you were in hot pursuit, with the numbers of applications that you would have to make and the time to make those, you could never catch up." *Foreign Intelligence Surveillance Act Reform: Hearing Before the H. Permanent Select Comm. On Intelligence*, 109th Cong. (July 19, 2006).
[37] Brief for Washington Legal Foundation as Amicus Curiae in Support of Defendants Urging Reversal, Am. Civil Liberties Union v. Nat'l Sec. Agency (Nos. 06-2095,06-2140), *available at* http://www.morgancunningham.net/downloads/article_38.pdf (emphasis in original).
[38] Telephone Interview with Mary DeRosa (Sept. 28, 2006).
[39] *FISA for the 21st Century: Hearings Before the S.Comm. on the Judiciary,* 109th Cong. (2006) [hereinafter *Hearings*] (Statement of Mary B. DeRosa, Senior Fellow, Center for Strategic and International Studies).
[40] *Id*.
[41] Response from Stephen Schulhofer, Robert B. McKay Professor of Law, New York University School of Law, to Center on Law & Security (Nov. 10, 2006).
[42] *Hearings, supra* note 39 (Statement of Bryan Cunningham, Principal, Morgan & Cunningham, LLC, former deputy legal advisor to the National Security Council under President George W. Bush).
[43] *Hearings, supra* note 39 (Statement of Mary B. DeRosa, Senior Fellow, Center for Strategic and International Studies).
[44] Telephone Interview with Mary DeRosa (Sept. 28, 2006).
[45] *Id*.
[46] Response from Stephen Schulhofer, Robert B. McKay Professor of Law, New York University School of Law, to Center on Law & Security (Nov. 10, 2006).
[47] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).
[48] *Id.* at 635.
[49] *Id.* at 637.
[50] Sense of Congress Regarding Terrorist Attacks, Pub. L. No. 107-40 (2001).
[51] See Letter from H. Bryan Cunningham, Attorney, Morgan & Cunningham, to Arlen Specter, Chair, Senate Judiciary Committee, and Patrick Leahy, Ranking Minority Member, Senate Judiciary Committee (Feb. 3, 2006), *available at* http://www.morgancunningham.net/downloads/article_22.pdf; *cf.* U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President *(Justice Dep't. White Paper of Jan. 19)* (2006), available at http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf [hereinafter *White Paper of Jan. 19*]; Brief for Washington Legal Foundation as Amicus Curiae in Opposition to Plaintiffs' Motion for Partial Summary Judgment and in Support of Defendants' Motion to Dismiss, or in the Alternative, for Summary Judgment, Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (2006) (No. 06-10204) [hereinafter *Amicus Brief]*.
[52] *Amicus Brief*, *supra* note 51.
[53] *White Paper of Jan. 19, supra* note 51.
[54] United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).
[55] *In re* Sealed Case, No. 02-001, 310 F.3d 717 (Fisa Ct. Rev. 2002).
[56] *White Paper of Jan. 19, supra* note 51.
[57] Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department White Paper of January 19, 2006 (February 2, 2006) [hereinafter Letter from Scholars].
[58] *Id*.
[59] J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc., 534 U.S. 124 (2001).
[60] Letter from Scholars, *supra* note 57.
[61] *Id.* (emphasis included in the original).
[62] *Id.* (citing Rasul v. Bush, 452 U.S. 466 (2004)).
[63] *Id.*
[64] *Id.*
[65] 126 S. Ct. 2749, 2755 (2006).
[66] Response from Stephen Schulhofer, Robert B. McKay Professor of Law, New York University School of Law, to Center on Law & Security (Nov. 10, 2006).
[67] Bamford, *supra* note 10.
[68] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts,* N.Y. Times, December 16, 2005, at A1. *See also* Carol D. Leonnig and Dafna Linzer, *Spy Court Judge Quits in Protest,* Washington Post, December 21, 2005, at A1; James Risen and Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. Times December 21, 2005, at A1.

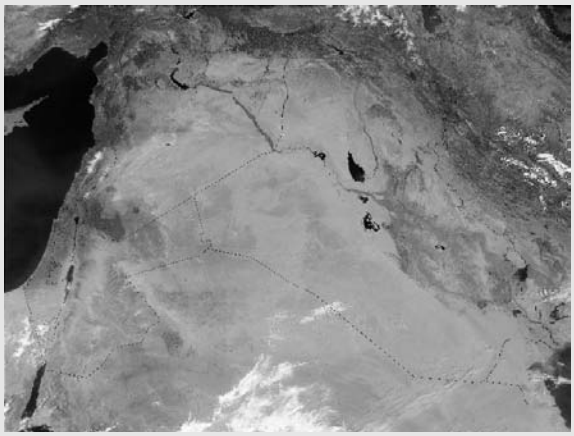


Image courtesy of MODIS Rapid Response Project at NASA/GSFC

Upcoming Conference at the Center on Law and Security

Iraq, Iran, & Beyond: America Faces the Future

The political landscape in the Middle East is in flux. Iran's influence seems to be ascendant, while the Taliban is regrouping in Afghanistan and Pakistan. Among the factors certain to shape the region in the years to come are the Sunni/Shiite divide, potential alliances among Muslim states, and U.S. foreign policy regarding Saudi Arabia and Syria.

Please join the Center on Law and Security as we discuss these issues and more at a full-day conference featuring **Center Fellow Peter Bergen, Steve Coll** of *The New Yorker*, **Jim Fallows** of *The Atlantic Monthly*, **Prof. Noah Feldman (NYU), Prof. Bernard Haykel (NYU), Prof. Farhad Kazemi (NYU), Col. W. Patrick Lang (Ret.)** of the U.S. Army, **Prof. Paul Pillar (Georgetown), Nir Rosen** of the New America Foundation, and **Center Fellow Lawrence Wright**.

Wednesday, January 24th, 2007 9 a.m. - 5 p.m.

Greenberg Lounge, NYU School of Law, 40 Washington Square South

For further information, call (212) 992-8854 or e-mail CLS@juris.law.nyu.edu

NYU Center on Law and Security

New York University School of Law
110 West Third Street
New York, NY 10012