UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CENTER FOR CONSTITUTIONAL RIGHTS, TINA M. FOSTER, GITANJALI S. GUTIERREZ, SEEMA AHMAD, MARIA LAHOOD, RACHEL MEEROPOL, Plaintiffs, v. GEORGE W. BUSH, President of the United States; NATIONAL SECURITY AGENCY, LTG Keith B. Alexander, Director; DEFENSE INTELLIGENCE AGENCY, LTG Michael D. Maples, Director; CENTRAL INTELLIGENCE AGENCY, Porter J. Goss, Director; DEPARTMENT OF HOMELAND SECURITY, Michael Chertoff, Secretary; FEDERAL BUREAU OF INVESTIGATION, Robert S. Mueller III, Director; JOHN D. NEGROPONTE, Director of National Intelligence, Defendants.	Case No. 06-cv-313 Judge Gerard E. Lynch Magistrate Judge Kevin N. Fox

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

William Goodman [WG-1241]
Shayana Kadidal [SK-1278]
Michael Ratner [MR-3357]
CENTER FOR CONSTITUTIONAL RIGHTS
666 Broadway, 7th Floor
New York, NY 10012-2317
(212) 614-6427

CCR Cooperating Counsel:
David Cole
c/o Georgetown University Law Center
600 New Jersey Avenue, N.W.
Washington, D.C. 20001
(202) 662-9078

Michael Avery
J. Ashlee Albies
NATIONAL LAWYERS GUILD
c/o Suffolk Law School
120 Tremont Street
Boston, MA 02108
(617) 573-8551

Attorneys for Plaintiffs

March 9, 2006

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Federal Statutes

INTRODUCTION

Plaintiffs seek summary judgment on their claims that the National Security Agency's (NSA) domestic spying program violates federal law, the separation of powers, and the First and Fourth Amendments. Defendants have admitted that they are conducting "electronic surveillance" as defined by the Foreign Intelligence Surveillance Act (FISA), that they are doing so without obtaining the court orders required by FISA, and that they have targeted phone calls and emails between persons outside the United States and persons within the United States where they believe that one of the communicants is associated with al Qaeda or unspecified associated groups. Because plaintiffs, in the course of their legal work, regularly communicate with persons outside the United States who are likely to fall within the range of persons targeted by the NSA spying program, they are unable to speak freely and confidentially in those communications, and seek injunctive relief to halt such surveillance as contrary to law.

The President's secret authorization of the NSA surveillance program, in direct contravention of two federal criminal statutes, reflects the kind of unilateral executive action that the framers of our Constitution sought to countermand through a system of checks and balances. The President has asserted that in the context of the "War on Terror," there are no checks and balances, because he has unilateral and unlimited power to choose "the means and methods of engaging the enemy." But as the Supreme Court stated less than two years ago, in rejecting similar Presidential assertions of uncheckable executive power to detain "enemy combatants," "a state of war is not a blank check for the President." *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) (plurality op). Federal statutes, the United States Constitution, and the rule of law itself require that the President be ordered to desist from exercising power that Congress has expressly

denied him, that violates First and Fourth Amendment rights, and that is not authorized by any provision of the Constitution.

STATEMENT OF UNDISPUTED FACTS

The following facts are undisputed. They rest entirely on the United States Code and public record legislative materials, public admissions of the defendants regarding the NSA spying program, and plaintiffs' descriptions of how defendants' actions have affected their conduct**.**

1. The Statutory Scheme

Electronic surveillance for foreign intelligence and national security purposes within the United States is regulated by the Foreign Intelligence Surveillance Act (FISA).[1] Congress enacted FISA in 1978 after revelations of widespread spying on Americans by federal law enforcement and intelligence agencies—including the NSA.[2] The Senate Judiciary Committee stated that the legislation was "in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."[3] FISA struck

---

[1] Pub. L. 95-511, 92 Stat. 1783 (1978), codified at 50 U.S.C. §§ 1801-62.

[2] A special congressional committee known as the Church Committee (after its Chairman, Sen. Frank Church) concluded, after lengthy investigation and hearings, "The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information – unrelated to any legitimate government interest – about the personal and political lives of American citizens. The collection of this type of information has in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials." Senate Comm. on the Judiciary, Foreign Intelligence Surveillance Act of 1977, S. Rep. No. 95-604, at 10, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3909 (citations omitted).

The Church Committee noted that Congress had "a particular obligation to examine the NSA, in light of its tremendous potential for abuse." Hearings Before the Select Committee To Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, Ninety-Four Congress, First Session, Volume 5, available at http://cryptome.org/nsa-4th.htm (Sen. Church).

In its final report, the Church Committee warned that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature." Intelligence Activities and the Rights of Americans, Book II, (Apr. 26, 1976) at 1, *available at* http://www.aarclibrary.org/publib/church/reports/book2/html/ChurchB2_0009a.htm.

[3] S. Rep. No. 95-604, at 7-8, 1978 U.S.C.C.A.N. at 3909.

a careful balance between protecting civil liberties and preserving the "vitally important government purpose" of obtaining valuable intelligence in order to safeguard national security.[4]

With minor exceptions not invoked by the administration and not relevant here, FISA authorizes "electronic surveillance" for foreign intelligence purposes only upon certain specified showings, and only if approved by a court. FISA governs only statutorily defined "electronic surveillance," principally surveillance targeted at U.S. citizens or permanent residents within the United States, or electronic surveillance gathered within the United States.[5] Accordingly, FISA leaves ungoverned interception abroad of a foreign target's electronic communications. "Electronic surveillance" governed by FISA is permissible upon a court order, which may issue based on a showing of probable cause that the target of the surveillance is an "agent of a foreign power," which includes a member of any "group engaged in international terrorism."[6] FISA does not require probable cause of criminal activity.

Congress sought to make crystal-clear that electronic surveillance was to be undertaken only pursuant to federal statute. To that end, Congress expressly provided that FISA and specified provisions of the federal criminal code (which govern wiretaps for criminal

---

[4] S. Rep. No. 95-604, pt. 1, at 9 (1977).

[5] FISA defines "electronic surveillance" in 50 U.S.C. § 1801(f) to include:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States…;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

[6] 50 U.S.C. § 1805(a) (court order); 1801(a)(4) (definition of foreign power includes organization engaged in international terrorism or activities in preparation therefor).

investigations) are the "*exclusive* means by which electronic surveillance … may be conducted."[7]

To underscore the point, Congress made it a crime—under two separate provisions of the United States Code—to undertake electronic surveillance not authorized by statute. FISA itself provides that it shall be a crime to conduct "electronic surveillance under color of law except as authorized by statute."[8] And Title 18 is even more explicit: 18 U.S.C. § 2511 makes it a crime to conduct wiretapping except as "*specifically provided in this chapter,"* § 2511(1), or as authorized by FISA, § 2511(2)(e).

Signing FISA into law, President Carter acknowledged that it applied to *all* electronic surveillance, stating: "The bill requires, for the first time, a prior judicial warrant for *all* electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign intelligence by electronic surveillance in the United States."[9]

In subjecting foreign intelligence electronic surveillance to strict statutory limits, FISA marked a substantial change in the law. Prior to FISA's enactment, Congress had chosen not to regulate foreign intelligence surveillance. In fact, when Congress regulated criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, it expressly recognized that it was leaving unregulated foreign intelligence surveillance:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, *to obtain*

---

7 18 U.S.C. § 2511(2)(f) (emphasis added)..

8 50 U.S.C. § 1809.

9 Foreign Intelligence Surveillance Act of 1978 *Statement on Signing S. 1566 Into Law,* 2 PUBLIC PAPERS 1853 (October 25, 1978) (papers of James E. Carter) (emphasis in original)

> *foreign intelligence information deemed essential to the security of the United States*, or to protect national security information against foreign intelligence activities.[10]

When Congress enacted FISA, however, it repealed the above provision, and substituted the language quoted above providing that FISA and Title III were the "exclusive means" for engaging in electronic surveillance and that any such surveillance conducted outside the authority of those statutes was not only prohibited, but a crime.

Most importantly for purposes of this case, Congress specifically addressed in FISA itself the question of domestic wiretapping during wartime. In 18 U.S.C. § 1811, entitled "Authorization during time of war," FISA dictates that "[n]otwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information *for a period not to exceed fifteen calendar days following a declaration of war by the Congress*."[11] Thus, even where Congress has declared war, the law limits warrantless wiretapping to the first fifteen days of the conflict. The legislative history of this provision explains that if the President needed further surveillance powers because of the special nature of the particular war at hand, fifteen days would be sufficient for Congress to consider and enact further statutory authorization.[12]

2. NSA Spying Program

In the fall of 2001, shortly after the terrorist attacks of September 11, the NSA launched a secret program to engage in electronic surveillance, without prior judicial authorization, of the

---

[10] 18 U.S.C. § 2511 (3) (1968).

[11] 50 U.S.C. § 1811 (emphasis added).

[12] "The Conferees intend that this [15-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency.... The conferees expect that such amendment would be reported with recommendations within 7 days and that each House would vote on the amendment within 7 days thereafter." H.R. Conf. Rep. No. 95-1720, at 34 (1978).

communications of persons inside the United States ("the Program").[13] Despite the clear intent of Congress that the President seek an amendment to FISA to authorize extraordinary surveillance during wartime, the President did not seek such an amendment, and instead acted unilaterally and in secret. President Bush has reauthorized the Program, again in secret, more than thirty times, and intends to continue doing so indefinitely.[14]

As part of the Program, the NSA targets for interception "calls ... [the government has] a reasonable basis to believe involve Al Qaida or one of its affiliates."[15] The NSA also targets the communications of individuals it deems suspicious on the basis of the NSA's belief that the targeted individuals have some unspecified "link" to al Qaeda or unspecified related terrorist organizations,[16] belong to an organization that the government considers to be "affiliated" with al

---

[13] President Bush, Radio Address (Dec. 17, 2005) (hereinafter *Bush Radio Address*), transcript available at: http://www.whitehouse.gov/news/releases/2005/12/20051217.html ("In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations."); James Taranta, *The Weekend Interview with Dick Cheney*, Wall Street Journal, Jan. 28-29, 2006, at A8 ("It the interception of communications, one end of which is outside the United States, and one end of which is, either outside the United States or inside."); Michael Hayden, *Remarks at the National Press Club on NSA Domestic Surveillance* (Jan. 23, 2006) (hereinafter *Hayden Press Club*) (acknowledging that the NSA Program covers "international calls"); Alberto Gonzales, *Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence*, Dec. 19, 2005 (hereinafter *Gonzales/Hayden Press Briefing*) ("The President has authorized a program to engage in electronic surveillance"); *Press Conference of President Bush*, December 19, 2005, transcript available at: http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html (noting that "calls" are intercepted).

[14] *Press Conference of President Bush*, December 19, 2005, available at: http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html ("I've reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for so long as our nation is—for so long as the nation faces the continuing threat of an enemy that wants to kill American citizens.").

[15] *Hayden Press Club*.

[16] *Bush Radio Address* ("Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks."); *Press Conference of President Bush*, December 19, 2005, transcript available at: http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html ("I authorized the interception of international communications of people with known links to al Qaeda and related terrorist organizations."); James Taranta, *The Weekend Interview with Dick Cheney*, Wall Street Journal, Jan. 28-29, 2006, at A8 ("It the interception of communications, ... one end of which ... we have reason to believe is al-Qaeda-connected."); "Ask the White House," Alberto Gonzales, Jan. 25, 2006, available at http://www.whitehouse.gov/ask/20060125.html (NSA intercepts "international communications involving someone we reasonably believe is associated with al Qaeda"); Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, Department of Justice, to congressional leaders, December 22, 2005 ("As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization.").

Qaeda,[17] have provided some unspecified support for al Qaeda,[18] or "want to kill Americans."[19] Information collected under the Program is sometimes retained and sometimes disseminated.[20] The Attorney General has refused to specify the number of Americans whose communications have been or are being intercepted under the Program.[21]

The NSA intercepts communications under the Program without obtaining a warrant or any other type of judicial authorization.[22] Nor does the President or the Attorney General

---

[17] Alberto Gonzales, *Gonzales/Hayden Press Briefing* ("[W]e have to have a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda.").

[18] *Id*.

[19] *Hayden Press Club* ("We are going after very specific communications that our professional judgment tells us we have reason to believe are those associated with people who want to kill Americans.").

[20] *Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006) (Attorney General Gonzales: "information is collected, information is retained and information is disseminated").

[21] Alberto Gonzales, *Gonzales/Hayden Press Briefing* ("QUESTION: General, are you able to say how many *Americans* were caught in this surveillance? ATTORNEY GENERAL GONZALES: I'm not -- *I can't get into the specific numbers because that information remains classified*. Again, this is not a situation where -- of domestic spying. *To the extent that there is a moderate and heavy communication involving an American citizen*, it would be a communication where the other end of the call is outside the United States and where we believe that either the American citizen or the person outside the United States is somehow affiliated with al Qaeda." (emphasis added)).

[22] Michael Hayden, *Gonzales/Hayden Press Briefing* ("The period of time in which we do this is, in most cases, far less than that which would be gained by getting a court order."); *Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006) (Attorney General Gonzales: "[T]he program is triggered [by] a career professional at the NSA."); *id.* ("QUESTION: Just to clarify sort of what's been said, from what I've heard you say today and an earlier press conference, *the change from going around the FISA law was to—one of them was to lower the standard from what they call for, which is basically probable cause to a reasonable basis; and then to take it away from a federal court judge, the FISA court judge, and hand it over to a shift supervisor at NSA. Is that what we're talking about here—just for clarification?* / GEN. HAYDEN: *You got most of it right.* The people who make the judgment, and the one you just referred to, there are only a handful of people at NSA who can make that decision. They're all senior executives, they are all counterterrorism and al Qaeda experts. So I—even though I—you're actually quoting me back, Jim, saying, "shift supervisor." To be more precise in what you just described, the person who makes that decision, a very small handful, senior executive. So in military terms, a senior colonel or general officer equivalent; and in professional terms, the people who know more about this than anyone else. / QUESTION: Well, no, that wasn't the real question. The question I was asking, though, was since you lowered the standard, doesn't that decrease the protections of the U.S. citizens? And number two, if you could give us some idea of the genesis of this. Did you come up with the idea? Did somebody in the White House come up with the idea? Where did the idea originate from? Thank you. / GEN. HAYDEN: Let me just take the first one, Jim. And I'm not going to talk about the process by which the President arrived at his decision. *I think you've accurately described the criteria under which this operates*, and I think I at least tried to accurately describe a changed circumstance, threat to the nation, and why this approach—limited, focused—has been effective." (emphasis added)); Alberto Gonzales, *Gonzales/Hayden Press Briefing* ("[T]he Supreme Court has long held that there are exceptions to the warrant requirement in—when special needs outside the law enforcement arena. And we think that that standard has been met here.").

authorize the specific interceptions.[23] Instead, an NSA "shift supervisor" is authorized to approve the selection of targets or of communications to be intercepted.[24]

Under the Program, communications are intercepted without probable cause to believe that the surveillance targets have committed or are about to commit any crime, or are foreign powers or agents thereof. Rather, the NSA intercepts communications when the agency has, in its own judgment, merely a "*reasonable basis to conclude* that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[25] Principal Deputy Director for National Intelligence (and former NSA Director) General Michael Hayden has admitted that "[t]he trigger is quicker and a bit softer than it is for a FISA warrant,"[26] and has suggested that the standard is "[i]nherent foreign intelligence value."[27] Attorney General Gonzales has conceded that the standard used is not criminal "probable cause."[28]

---

[23] *Hayden Press Club* ("These are communications that we have reason to believe are Al Qaida communications: a judgment made by American intelligence professionals, not folks like me or political appointees.").

[24] Michael Hayden, *Gonzales/Hayden Press Briefing* (explaining that the judgment to target a communication "is made by the operational work force at the National Security Agency using the information available to them at the time, and the standard that they apply—and it's a two-person standard that must be signed off by a shift supervisor, and carefully recorded as to what created the operational imperative to cover any target, but particularly with regard to those inside the United States"); *see also Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006) (Attorney General Gonzales: "The decision as to which communications will be surveilled are made by intelligence experts out at NSA.").

[25] Alberto Gonzales, *Gonzales/Hayden Press Briefing* (emphasis added); *see also Hayden Press Club* (explaining that the NSA intercepts calls "we have a reasonable basis to believe involve Al Qaida or one of its affiliates").

[26] *Hayden Press Club.*

[27] *Hayden Press Club* ("Inherent foreign intelligence value is one of the metrics we must use to ensure that we conform to the Fourth Amendment's reasonableness standard when it comes to protecting the privacy of these kinds of people.").

[28] *Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006) (Attorney General Gonzales: "I think it's probable cause. But it's not probable cause as to guilt… Or probable cause as to a crime being committed. It's probable cause that a party to the communication is a member or agent of Al Qaida. The precise language that I'd like to refer to is, 'There are reasonable grounds to believe that a party to communication is a member or agent or Al Qaida or of an affiliated terrorist organization.' It is a probable cause standard, in my judgment.").

The Program intercepts communications that are subject to the requirements of FISA. FISA states that "[a] person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. § 1809. The Attorney General has admitted that the Program constitutes "electronic surveillance" as defined in and governed by FISA:

> Now, in terms of legal authorities, the Foreign Intelligence Surveillance Act provides—requires a court order before engaging in this kind of surveillance that I've just discussed and the President announced on Saturday, unless there is somehow—there is—unless otherwise authorized by statute or by Congress. That's what the law requires.[29]

Nonetheless, the Program has been used "in lieu of" the procedures specified under FISA.[30] In the words of General Michael Hayden, the Principal Deputy Director for National Intelligence, "this is a more ... 'aggressive' program than would be traditionally available under FISA."[31]

The administration considered asking Congress to amend FISA to permit the NSA spying program, but elected not to do so, and instead ordered its implementation in secret. Attorney General Gonzales acknowledged that administration officials consulted various members of

---

[29] Alberto Gonzales, *Gonzales/Hayden Press Briefing.*

[30] Michael Hayden, *Gonzales/Hayden Press Briefing*; *see also Hayden Press Club* ("If FISA worked just as well, why wouldn't I use FISA? To save typing? No. There is an operational impact here, and I have two paths in front of me, both of them lawful, one FISA, one the Presidential—the President's authorization. And we go down this path because our operational judgment is it is much more effective. So we do it for that reason."); Michael Hayden, *Gonzales/Hayden Press Briefing* ("What you're asking me is, can we do this program as efficiently using the one avenue provided to us by the FISA Act, as opposed to the avenue provided to us by subsequent legislation and the President's authorization. Our operational judgment, given the threat to the nation that the difference in the operational efficiencies between those two sets of authorities are such that we can provide greater protection for the nation operating under this authorization.").

[31] Michael Hayden, *Gonzales/Hayden Press Briefing*; *see also Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006). (Attorney General Gonzales: "In the instances where this program applies, FISA does not give us the operational effect that the authorities that the President has given us give us."); Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, Department of Justice, to congressional leaders, December 22, 2005 ("[T]he President determined that it was necessary following September 11 to create an early warning detection system. FISA could not have provided the speed and agility required for the early warning detection system.").

Congress about seeking legislation to authorize the Program but ultimately chose not to do so because they were advised that it would be "difficult if not impossible" to obtain.[32]

3. Plaintiffs' Injuries

Plaintiffs are the Center for Constitutional Rights, a national non-profit public interest law firm, and some of its lawyers and legal staff. CCR has filed several lawsuits against administration measures undertaken in the "War on Terror" that violate statutory, constitutional and international human rights. In the course of that litigation and related work, CCR lawyers and legal staff communicate regularly with persons outside the United States who defendants have asserted are associated with al Qaeda or associated groups. They often communicate by telephone and email, as those are the most efficient ways to do so. In addition, some of plaintiffs' clients are barred from entering the United States.

For example, plaintiffs represent Maher Arar, a Canadian citizen suing the United States and various federal officials for stopping him while he was changing planes at JFK airport and ordering him removed to Syria, where he was tortured and detained without charges for nearly a year. *Arar v. Ashcroft*, No. CV-04-0249 (DGT) (VVP), 2006 U.S. Dist. LEXIS 5803 (E.D.N.Y. Feb 16, 2006). Syria released Arar after a year, stating that it found no basis for charging him with a crime. He is a free man in Canada, which also has not charged him with any crime. The United States asserts that Arar is associated with al Qaeda, a charge Arar denies. But given that assertion, Arar fits squarely within the category of persons defendants have admitted are subject to NSA surveillance. Plaintiffs also represent several former Guantánamo detainees who are also viewed by the government as fitting within the category of persons subject to NSA surveillance

[32] Attorney General Gonzales stated, "We have had discussions with Congress in the past—certain members of Congress—as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, and we were advised that that would be difficult, if not impossible." *Gonzales/Hayden Press Briefing*.

program. *See* Affirmation of William Goodman at ¶¶ 10, 6-7. And as part of their legal work, plaintiffs speak regularly with other witnesses and potential clients who may also fall within the government's broad category of persons subject to NSA spying. *Id*.

Plaintiffs must now assume that their clients—and others with whom they communicate in connection with their legal representation—are being subject to electronic surveillance. This makes it impossible to conduct confidential communications with those persons by telephone or email. Accordingly, plaintiffs must seek out far less efficient and more costly ways of communicating where confidences are critical, including traveling abroad, the U.S. mails, or other couriers. *See id.* at ¶ 15. Plaintiffs have had to review and analyze all past international communications in order to evaluate whether confidences may have been breached by Defendants' illegal surveillance and whether measures ought to be taken in response. *Id*. at ¶ 16. Plaintiffs have also sought disclosure of whether privileged communications were subject to surveillance under the Program. *See id*. at ¶ 13 (describing interrogatories submitted on Feb. 22, 2006 in *Turkmen v. Ashcroft*, No. 02-CV-2307 (E.D.N.Y.)).

SUMMARY OF ARGUMENT

The NSA surveillance program violates federal statutes and the Constitution, and therefore should be enjoined. First, it violates two federal criminal statutes prohibiting electronic surveillance except pursuant to FISA or Title III of the criminal code. 50 U.S.C. § 1809; 18 U.S.C. § 2511. Congress made clear that even when it has declared war—a much more grave act than authorizing the use of military force—warrantless wiretapping of Americans is permissible only for the first fifteen days of the conflict, and is a crime thereafter. Here, Congress has not declared war, and the NSA spying program has gone on for more than four years. The

administration's argument that Congress somehow authorized limitless warrantless wiretapping without saying so in the Authorization to Use Military Force against al Qaeda cannot be squared with the express terms of FISA and 18 U.S.C. § 2511.

Second, because the President acted in direct contravention of two federal statutes, and because he does not have unilateral, uncheckable authority to wiretap Americans at home, even in wartime, his actions also violate the separation of powers. When the President acts contrary to Congressional will, his power is at its "lowest ebb," and his actions may be upheld "only by disabling Congress from acting upon the subject." *Youngstown Sheet & Tube v. Sawyer*, 343 U.S. 579, 638-39 (1952) (Jackson, J., concurring). Congress plainly has authority to enact laws protecting the privacy of American's electronic communications, and may not be disabled from acting upon the subject. Therefore, the President's actions violate the separation of powers.

Third, the NSA program violates the First and Fourth Amendments, because it intrudes directly upon speech that has a reasonable expectation of privacy, and does so without obtaining a court order. Since the Supreme Court first extended Fourth Amendment protections to telephone calls in 1967, it has never upheld wiretapping on anything less than a warrant supported by probable cause. The NSA program, which eschews the warrant requirement altogether, accordingly violates the Fourth Amendment. And because it directly infringes First Amendment speech and association rights in doing so, it also violates the First Amendment.

ARGUMENT

I. Summary Judgment is Appropriate Based on Defendants' Admissions about the Scope of the NSA Spying Program, Which Establish on Their Face That the NSA Spying Program Violates Federal Statutes and the Constitution

The only facts necessary to resolve this dispute have been admitted by defendants. They have admitted that the NSA spying program exists, that it consists of "electronic surveillance" that

would otherwise be covered by FISA, and that it monitors calls and emails between persons outside the United States and persons inside the United States, where the government has reason to believe that one of the persons is associated with al Qaeda or unspecified groups supportive of al Qaeda, or otherwise fits its open-ended criteria for targeting. In addition, defendants have admitted that they conduct the surveillance without judicial approval in the form of a court order.

Those facts are sufficient to establish a case or controversy. Plaintiffs have suffered injury by the existence of the NSA spying program, because they have a reasonable fear that their communications have been and will continue to be illegally monitored under the auspices of the program. In the course of their legal representation, they communicate regularly with persons outside the United States, such as Maher Arar, whom the government views as falling within the terms of the program described by the Attorney General. The fact that their attorney-client and attorney work product communications are likely to be overheard by the government—the defendant in many of the lawsuits plaintiffs have filed—means that plaintiffs cannot engage in confidential communications with their clients and others. Plaintiffs have already taken objective measures to respond to these concerns.[33]

As set forth below, plaintiffs maintain that the NSA spying program violates federal law and the Constitution, and is therefore "contrary to law" and subject to injunctive relief under the Administrative Procedure Act. *See* 5 U.S.C. § 706(2)(A), § 706(2)(C) (a court shall "hold

[33] *See* Affirmation of William Goodman at ¶¶ 13-16, 19. It is well-established that plaintiffs may challenge government action that has a chilling effect on their First Amendment rights even where the action has not been applied to them, so long as they have a credible fear that the government will take action against them, and their conduct makes it reasonable to believe that they will be affected. *See, e.g.*, *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979); *Virginia v. American Booksellers Ass'n*, 484 U.S. 383 (1988); *Meese v. Keene*, 481 U.S. 465 (1987); *Latino Officers Ass'n v. Safir*, 170 F.3d 167, 170 (2d Cir. 1999); *Nitke v. Ashcroft*, 253 F. Supp. 2d 587, 598 (S.D.N.Y. 2003). Plaintiffs have alleged that their communications fall within the exact terms set forth by defendants regarding the scope of this program, and that they have a continuing and pressing need to engage in such communications with assurances of confidentiality. That is sufficient to ground standing to sue.

unlawful and set aside agency action" that is "otherwise not in accordance with law, " that is taken "in excess of statutory ... limitations," or "in excess of statutory ... authority.").

II. The NSA Spying Program Violates FISA

Congress made it clear in FISA and 18 U.S.C. § 2511 that foreign intelligence electronic surveillance must be conducted pursuant to statute, and pursuant to court order. It underscored that intention by making wiretapping without statutory authorization a crime. 50 U.S.C. § 1809; 18 U.S.C. § 2511. And Congress expressly provided that even when it has declared war—a step it did not take with respect to al Qaeda—the President is limited to fifteen days of warrantless wiretapping of Americans, and must seek a statutory amendment if he believes any further warrantless electronic surveillance is necessary. 50 U.S.C. § 1811. *See generally* Statement of Facts, *supra.*

In the face of these specific legislative directives, President Bush declined to ask Congress to amend FISA to permit the NSA spying program to go forward. He did seek other amendments to FISA in the immediate aftermath of the terrorist attacks of September 11, 2001, in what ultimately became the USA PATRIOT Act. But he chose not to ask Congress for an amendment to approve of the NSA spying program, and instead unilaterally ordered that the program be adopted in secret. On its face, because the NSA program conducts "electronic surveillance" outside of the process carefully prescribed by FISA, it violates FISA and 18 U.S.C. § 2511, and is contrary to law.[34]

The administration has argued that Congress, without ever saying so, authorized the NSA spying program when, on September 18, 2001, it enacted the Authorization to Use Military

[34] The Congressional Research Service has independently found that the NSA program violates federal law. *See* Congressional Research Service, "Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information" (Jan. 5, 2006).

Force (AUMF) against the perpetrators of 9/11 and those who harbor them.[35] This argument fails for three reasons: (1) it is directly contradicted by specific language in other federal statutes establishing that FISA and the criminal code are the "exclusive means" for conducting electronic surveillance; (2) it would require a repeal by implication of those statutes, and there is no basis for overcoming the strong presumption against implied repeals here; and (3) it conflicts with the administration's claim that it chose not to ask Congress to amend FISA to authorize the program because several members of Congress told them that it would be "difficult, if not impossible" to obtain.

A. The AUMF's General Authorization to Use All Necessary and Appropriate Force against Al Qaeda Does Not Override Congress's Specific Restrictions on Wiretapping Americans.

In FISA, Congress directly and specifically regulated domestic warrantless wiretapping for foreign intelligence and national security purposes, including during wartime. The administration's argument that the AUMF somehow trumps FISA would require the Court to override FISA's express and specific language based on an unstated general "implication" from the AUMF. But it is well established that specific and "carefully drawn" statutes prevail over general statutes where there is a conflict.[36] As such, FISA clearly governs here.

In light of Congress's specific regulation of electronic surveillance in FISA, and in particular its proviso that even a declaration of war authorizes no more than fifteen days of warrantless wiretapping, there is simply no basis for finding in the AUMF's general language implicit authority for unchecked warrantless domestic wiretapping. Neither the text of the

---

[35] Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001). The Department of Justice has set forth in detail its defense of the NSA program in Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) (hereinafter "DOJ Memo"), available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

[36] *Morales v. TWA, Inc.*, 504 U.S. 374, 384-85 (1992) (quoting *International Paper Co. v. Ouelette*, 479 U.S. 481, 494 (1987)).

AUMF nor its legislative history contains one word about authorizing surveillance, much less warrantless surveillance of Americans at home. As Justice Frankfurter stated in rejecting a similar argument by President Truman when he sought to defend the seizure of the steel mills during the Korean War on the basis of implied congressional authorization:

> It is one thing to draw an intention of Congress from general language and to say that Congress would have explicitly written what is inferred, where Congress has not addressed itself to a specific situation. It is quite impossible, however, when Congress did specifically address itself to a problem, as Congress did to that of seizure, to find secreted in the interstices of legislation the very grant of power which Congress consciously withheld. To find authority so explicitly withheld is … to disrespect the whole legislative process and the constitutional division of authority between President and Congress.[37]

Since Congress specifically provided that even a declaration of war—a more formal step than an authorization to use military force—would authorize only fifteen days of warrantless surveillance, one cannot reasonably conclude that the AUMF provides the President with *unlimited and indefinite* warrantless wiretapping authority.

The administration has invoked *Hamdi v. Rumsfeld,*[38] arguing that since the Supreme Court in that case construed the AUMF to provide sufficient statutory authorization for detention of American citizens captured on the battlefield in Afghanistan, the AUMF may also be read to authorize the President to conduct "signals intelligence" on the enemy, even if that includes electronic surveillance targeting U.S. persons within the United States. But there are two dispositive differences between this case and *Hamdi*. First, warrantless wiretapping of Americans at home is far less clearly within the ambit of implied war powers than the power to detain an enemy soldier on a foreign battlefield. [39] And second, FISA specifically addresses

---

[37] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 609 (1952) (Frankfurter, J., concurring).

[38] 542 U.S. 507 (2004).

[39] The Department of Justice argues that signals intelligence, like detention, is a "fundamental incident of waging war," and therefore is authorized by the AUMF. DOJ Memo at 12-13. But what is properly considered an implied incident of conducting war is affected by the statutory landscape that exists at the time the war is authorized.

wiretapping authority during wartime. 50 U.S.C. § 1811. By contrast, in *Hamdi,* Congress had not specifically enacted a statute authorizing limited detention of American citizens during wartime, and therefore the Court was free to read the AUMF to authorize detention of U.S. citizens captured fighting for the enemy on a foreign battlefield. Had there been a statute on the books providing that when Congress declares war, the President may detain Americans as "enemy combatants" *only* for the first fifteen days of the conflict, the Court could not reasonably have read the AUMF to authorize silently what Congress had specifically sought to limit.

Recognizing the problem 50 U.S.C. § 1811 poses for its statutory argument, the administration has argued that the AUMF might convey more authority than a declaration of war, noting that a declaration of war is generally only a single sentence.[40] But in fact, *every* declaration of war has been accompanied, *in the same enactment*, by an authorization to use military force.[41] It would be senseless to declare war without authorizing the President to use military force in the conflict. In light of that reality, § 1811 necessarily contemplates a situation in which Congress has both declared war *and* authorized the use of military force—and even that double authorization permits only fifteen days of warrantless electronic surveillance. Where, as here, Congress has seen fit only to authorize the use of military force—and not to declare war—

Thus, even if warrantless electronic surveillance *of Americans* for foreign intelligence purposes were a traditional incident of war when that subject was unregulated by Congress—which is far from obvious, at least in cases where the Americans targeted are not themselves suspected of being foreign agents or in league with terrorists—it can no longer be an implied incident after the enactment of FISA, which expressly addresses the situation of war, and precludes such conduct beyond the first fifteen days of the conflict.

[40] DOJ Memo at 26-27.

[41] *See* Declaration against the United Kingdom, 2 Stat. 755 (June 18, 1812) (War of 1812); Recognition of war with Mexico, 9 Stat. 9-10 (May 13, 1846) (Mexican-American War); Declaration against Spain, 30 Stat. 364 (Apr. 25, 1898) (Spanish-American War); Declaration against Germany, 40 Stat. 1 (Apr. 6, 1917) (World War I); Declaration against the Austro-Hungarian Empire, 40 Stat. 429 (Dec. 7, 1917) (same); Declaration against Japan, 55 Stat. 795 (Dec. 8, 1941) (World War II); Declaration against Germany, 55 Stat. 796 (Dec. 11, 1941) (same); Declaration against Italy, 55 Stat. 797 (Dec. 11, 1941) (same); Declarations against Bulgaria, Hungary, and Rumania, 56 Stat. 307 (June 5, 1942) (same).

the President cannot assert that he has been granted *more* authority than when Congress declares war as well.

The argument that the AUMF somehow amended FISA belies any reasonable understanding of legislative intent. An amendment to FISA of the sort that would be required to authorize the NSA program would be a momentous statutory development, undoubtedly subject to serious legislative debate. It is decidedly *not* the sort of thing that Congress would enact *inadvertently, and without even mentioning the fact.* As the Supreme Court recently noted, "'Congress … does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.'" *Gonzales v. Oregon*, 126 S. Ct. 904, 921 (2006) (quoting *Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001)).

B. The AUMF Cannot be Interpreted to Implicitly Repeal 18 USC § 2511.

Defendants have conceded that their statutory authorization argument based on the AUMF would require the conclusion that Congress implicitly repealed several sections of 18 U.S.C. § 2511. *See* DOJ Memo at 36 n.21. Section 2511(2)(f) identifies FISA and specific criminal code provisions as "the *exclusive* means by which electronic surveillance ... may be conducted." In addition, Section 2511 makes it a crime to conduct wiretapping except as "*specifically provided in this chapter,"*[42] or as authorized by FISA.[43] The AUMF is neither "in this chapter" (*i.e*. part of Title III, the 1968 Wiretap Act) nor an amendment to FISA, and therefore to find it to authorize electronic surveillance would require an implicit repeal of all the above provisions of 18 U.S.C. § 2511.

---

[42] 18 U.S.C.§ 2511(1).

[43] *Id.* § 2511(2)(e).

Repeals by implication are strongly disfavored; they can be established only by "overwhelming evidence" that Congress intended the repeal.[44] Here, there is no such evidence. "'[T]he only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable.'"[45] Section 2511 and the AUMF are fully reconcilable. The former makes clear that specified existing laws are the "exclusive means" for conducting electronic surveillance, and that conducting wiretapping outside that specified legal regime is a crime. The AUMF authorizes only such force as is "necessary and *appropriate*." There is no evidence that Congress considered tactics violative of existing express statutory limitations to be "appropriate." Accordingly, there is no basis whatsoever, let alone the "overwhelming evidence" required, for overcoming the strong presumption against implied repeals.

C. The Administration's Explanation for Why It Did Not Ask Congress to Approve the NSA Spying Program and Subsequent Actions Contradict Its Contention That Congress Approved the Program without Saying So

The administration's own statements and actions contradict its claim that the AUMF afforded it authority to conduct warrantless wiretaps. As noted above, Attorney General Alberto Gonzales admitted that the administration did not seek to amend FISA to authorize the NSA spying program because some members of Congress advised the administration that it would be "difficult, if not impossible to do so."[46] The administration cannot argue on the one hand that Congress authorized the NSA program in the AUMF, and at the same time that it did not ask Congress for such authorization because it would be "difficult, if not impossible" to get it.

The administration's actions vis-à-vis actual and proposed legislation also contradict their current assertion that the AUMF authorized warrantless wiretapping of Americans. Five weeks

---

44 *J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc.*, 534 U.S. 124, 137 (2001).

45 *Id.* at 141-142 (quoting *Morton v. Mancari*, 417 U.S. 535, 550 (1974)).

46 *Gonzales/Hayden Press Briefing, supra* note 13.

after the AUMF was signed, on October 26, 2001, Congress explicitly amended FISA in several respects when it passed the USA PATRIOT Act.[47] Congress subsequently amended FISA again two months later, extending from 24 to 72 hours the emergency warrant provision of 18 U.S.C. § 1805(f).[48] In doing so Congress specifically found that the 72-hour period was adequate for the preparation of FISA warrant applications in emergency conditions.[49] Yet there would have been little need for these amendments if the AUMF had already given the President the power to conduct unlimited warrantless electronic surveillance in terrorism cases. Nor was there any discussion in Congress at the time the PATRIOT Act was passed, or when FISA was subsequently amended further, acknowledging the administration's view that the AUMF made FISA irrelevant for a whole category of foreign intelligence electronic surveillance. These amendments of FISA undercut the contention that the President had already been given even broader powers under the AUMF.

In addition, one of the amendments the administration was contemplating seeking in 2002, in a draft bill leaked to the press entitled the "Domestic Security Enhancement Act of 2003," would have amended 50 U.S.C. § 1811 to extend its fifteen-day authorization for warrantless wiretapping to situations where Congress had not declared war but only authorized use of military force, or where the nation had been attacked.[50] If, as the administration now

---

[47] Pub. L. No. 107-56, 115 Stat. 272, §§ 206, 207, 208, 214, 215, 218, 504, 1003 (Oct. 26, 2001) (all sections amending FISA in some respect).

[48] Intelligence Authorization Act for Fiscal Year 2002, Pub. L. 107-108, 115 Stat. 1394, § 314(a)(2)(B) (Dec. 28, 2001).

[49] The House and Senate Conference Committee found, "The conferees agreed to a provision to extend the time for judicial ratification of an emergency FISA surveillance or search from 24 to 72 hours. That would give the Government adequate time to assemble an application without requiring extraordinary effort by officials responsible for the preparation of those applications." H.R. Conf. Rep. 107-328, H.R. Conf. Rep. No. 328, 107th Cong., 1st Sess. 2001 at 23, 2002 U.S.C.C.A.N. 1217, 1224.

[50] *See* Domestic Security Enhancement Act of 2003, § 103 (Strengthening Wartime Authorities Under FISA) (draft Justice Dept bill), available at *http://www.pbs.org/now/politics/patriot2-hi.pdf.*

contends, the AUMF gave the President unlimited authority to conduct warrantless wiretapping of the enemy, it would make no sense to seek such an amendment.

For these reasons, the Court should find that the NSA spying program violates FISA and 18 USC § 2511, and should enjoin the program as contrary to law.

III. The NSA Spying Program Violates the Separation of Powers Because Article II Does Not Empower the President to Violate FISA

The NSA spying program also violates the separation of powers. Wiretapping Americans, even during wartime, is not an exclusive executive prerogative immune from regulation by the other branches. Through FISA, foreign intelligence wiretapping has been subject to legislative and judicial checks for nearly thirty years, and its constitutionality in so restricting the executive has not previously been challenged. Because the President acted in contravention of FISA's express limits, his constitutional power is at its "lowest ebb," and he may act in contravention of statute only if Congress may be "disable[ed] ... from acting upon the subject" of foreign intelligence electronic surveillance within the United States. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). In fact, Congress acted well within its Article I powers in regulating executive intrusions on the privacy of U.S. persons in international electronic communications, and did not intrude on the President's Article II role. Accordingly, the President's actions violate the separation of powers.

A. The President Does Not Have Exclusive Authority to Wiretap Americans without a Warrant in Contravention of a Federal Statute Prohibiting that Conduct.

The administration has argued that the President has exclusive constitutional authority over "the means and methods of engaging the enemy," and that therefore FISA is

unconstitutional if it prohibits warrantless "electronic surveillance" deemed necessary by the President in the conflict with al Qaeda.[51] The argument that conduct undertaken by the Commander in Chief that has some relevance to "engaging the enemy" is immune from congressional regulation is directly contradicted by both case law and historical precedent. Every time the Supreme Court has confronted a statute limiting the Commander in Chief's authority, it has upheld the statute. No precedent holds that the President, when acting as Commander in Chief, is free to disregard an act of Congress designed specifically to restrain the President.

Analysis of the separation of powers question presented by the NSA spying program is governed by *Youngstown Sheet & Tube Co.*, 343 U.S. 579 (1952), and particularly by Justice Jackson's influential concurring opinion therein. In that case, the Supreme Court held that President Truman had no implied constitutional power as Commander in Chief to seize American steel companies to assure the production of materials necessary to prosecute the Korean War, because Congress had considered and rejected giving him authority to do so. In his concurring opinion, Justice Jackson analyzed three different situations in which the President might attempt to exercise implied power under the Constitution: (1) Presidential action pursuant to an express or implied authorization by Congress, in which case Presidential authority is at is maximum; (2) Presidential action in the face of Congressional silence, which Justice Jackson characterized as a "zone of twilight"; and (3) Presidential action contrary to the expressed or implied will of Congress, in which case Presidential power is at "its lowest ebb." 343 U.S. at 636-38.

The NSA spying program falls within Justice Jackson's third category, because FISA expressly required individualized judicial approval of foreign intelligence electronic surveillance

[51] DOJ Memo at 6-10, 28-36.

of the type involved in the NSA spying program, and made it a crime to engage in electronic surveillance without statutory authority. Accordingly, the President's power is at its lowest ebb, and his actions may be sustained only "by disabling the Congress from acting upon the subject." *Id.*

There is no doubt that Presidents have routinely collected signals intelligence on the enemy during wartime. Indeed, for most of our history Congress did not regulate foreign intelligence gathering in any way. But as Justice Jackson made clear in *Youngstown*,[52] to say that a President may undertake certain conduct in the absence of contrary congressional action does not mean that he may undertake that action where Congress has addressed the issue and disapproved of the action. Here, Congress has not only disapproved of the action the President has taken, but made it a crime.

The only question, then, is whether Congress is "disabled from acting upon the subject." *Youngstown*, 343 U.S. at 637-38. There can be no serious dispute that Congress's Article I powers afford it the authority to regulate wiretapping of U.S. persons on American soil. And the Supreme Court in *United States v. United States District Court (Keith)* expressly held that Congress had the power to set forth reasonable standards governing the warrant process for domestic national security surveillance:

> We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

United States v. United States District Court (Keith), 407 U.S. 297, 323-24 (1972). As Congress

---

[52] 343 U.S. at 635-38 (Jackson, J., concurring).

properly recognized in enacting FISA,[53] "even if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance for foreign intelligence purposes, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted."[54] This analysis was "supported by two successive Attorneys General."[55]

The President's broad assertion of uncheckable authority to choose the "means and methods of engaging the enemy" finds no support in the case law, the text of the Constitution, or the history of executive-legislative interactions during wartime. Every time the Supreme Court has addressed the propriety of executive action contrary to congressional statute during wartime, it has required the President to adhere to legislative limits on his authority. In *Youngstown*, as

---

[53] Indeed, Congress modeled FISA along lines suggested by the Supreme Court in *Keith*, 407 U.S. at 322-24 ("Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. ... the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection ... It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (*e.g.*, the District Court for the District of Columbia or the Court of Appeals for the District of Columbia Circuit); and that the time and reporting requirements need not be so strict as those in § 2518.").

[54] H.R. Rep. No. 95-1283, pt. 1, at 24 (1978) (emphasis added).

[55] *Id.* *See also* S. Rep. No. 95-604, pt. I, at 16 (1977) (Congress's assertion of power to regulate the President's authorization of electronic surveillance for foreign intelligence purposes was "concurred in by the Attorney General*"); Foreign Intelligence Electronic Surveillance: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess., at 31 (1978) (Letter from John M. Harmon, Assistant Attorney General, Office of Legal Counsel, to Edward P. Boland, Chairman, House Permanent Select Comm. on Intelligence (Apr. 18, 1978)) ("it seems unreasonable to conclude that Congress, in the exercise of its powers in this area, may not vest in the courts the authority to approve intelligence surveillance"). Attorney General Griffin Bell supported FISA in part because "no matter how well intentioned or ingenious the persons in the Executive branch who formulate these measures, the crucible of the legislative process will ensure that the procedures will be affirmed by that branch of government which is more directly responsible to the electorate." *Foreign Intelligence Surveillance Act of 1978: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. On Intelligence*, 95th Cong., 2d Sess. 12 (1977).

President Ford's Attorney General Edward Levi, testifying before a Senate Judiciary subcommittee in support of FISA, stated: "I really cannot imagine a President, if this legislation is in effect, going outside the legislation for matters which are within the scope of this legislation. …because I really do not think its is quite appropriate to describe the Presidential authority as being absolute on the one hand, or nonexistent on the other….there is a middle category where, assuming Presidential authority, that authority nevertheless, can be directed by the Congress." *Hearing before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, United States Senate*, 94th Cong., 2d Sess. (Mar. 29-30, 1976).

noted above, the Court invalidated President Truman's wartime seizure of the steel mills, where Congress had "rejected an amendment which would have authorized such governmental seizures in cases of emergency."[56]

In *Little v. Barreme*,[57] the Court held unlawful a seizure pursuant to Presidential order of a ship during the "Quasi War" with France. The Court found that Congress had authorized the seizure only of ships going *to* France, and therefore the President could not unilaterally order the seizure of a ship coming *from* France. Just as in *Youngstown*, the Court invalidated executive action taken during wartime, said to be necessary to the war effort, but implicitly disapproved by Congress.[58]

President Bush's unilateral executive action with respect to the NSA is more sharply in conflict with congressional legislation than the Presidential actions in either *Youngstown* or *Barreme*. In those cases, Congress had merely failed to give the President the authority in question, and thus the statutory limitation was *implicit*. Here, Congress went further, and *expressly prohibited* the President from taking the action in question. And it did so in the strongest way possible, by making the conduct a crime.

More recent Supreme Court decisions, in the context of the current conflict with al Qaeda, reaffirm the teachings of *Youngstown* and *Barreme*. In *Rasul v. Bush*, 542 U.S. 466 (2004), the administration maintained that it would be unconstitutional to interpret the habeas

---

[56] 343 U.S. 579, 586 (1952); *see also id.* at 597-09 (Frankfurter, J., concurring); *id.* at 656-60 (Burton, J., concurring); *id.* at 662-66 (Clark, J., concurring in the judgment).

[57] 6 U.S. (2 Cranch) 170 (1804).

[58] Similarly, in *Ex parte Milligan*, 71 U.S. (4 Wall.) 2 (1866), the Court unanimously held that the Executive violated the Habeas Corpus Act of March 3, 1863, 12 Stat. 696, by failing to discharge from military custody a petitioner held by order of the President and charged with, inter alia, affording aid and comfort to rebels, inciting insurrection, and violation of the laws of war. *See id.* at 115-117, 131 (majority opinion); *id.* at 133-136 (Chase, C.J., concurring); *see also id*. at 133 (noting that "[t]he constitutionality of this act has not been questioned and is not doubted," even though the act "limited this authority [of the President to suspend habeas] in important respects"). *See also Ex parte Endo*, 323 U.S. 214 (1944) (finding that President had no authority to detain loyal U.S. citizen during war where Congress had not authorized it).

corpus statute to afford judicial review to enemy combatants held at Guantánamo Bay because it "would directly interfere with the Executive's conduct of the military campaign against al Qaeda and its supporters," and would raise "grave constitutional problems."[59] The six-justice majority refused to accept this argument, and held that Congress had conferred habeas jurisdiction on the federal courts to entertain the detainees' habeas actions. Justice Scalia, writing for the three dissenters, agreed that Congress *could have* extended habeas jurisdiction to the Guantánamo detainees, and differed only as to whether Congress had in fact done so.[60] Thus, not a single Justice accepted the Bush administration's contention that the President's role as Commander in Chief may not be limited by congressional and judicial oversight.

Similarly, in *Hamdi v. Rumsfeld*, the Court rejected the President's argument that courts may not inquire into the factual basis for the detention of a U.S. citizen as an enemy combatant. As Justice O'Connor wrote for the plurality, "[w]hatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake."[61]

Detaining enemy combatants captured on the battlefield is surely closer to the core of "engaging the enemy" than is warrantless wiretapping of U.S. persons within the United States. Yet the Supreme Court in the enemy combatant cases squarely held that Congress and the courts both had a proper role to play in reviewing and restricting the President's detention power. These cases thus refute the administration's contention that Congress may not enact statutes that regulate and limit the President's choices of the "means and methods of engaging the enemy" as Commander in Chief.

---

[59] Brief for Respondents at 42, 44, *Rasul v. Bush* (Nos. 03-334, 03-343).
[60] *Rasul*, 542 U.S. at 506 (Scalia, J., dissenting).
[61] 542 U.S. 507, 536 (2004).

The Constitution's text confirms this conclusion. The framers of the Constitution made the President the "Commander in Chief," but otherwise assigned substantial power to Congress in connection with warmaking. Article I gives Congress the power to declare war and to authorize more limited forms of military enterprises (through "letters of marque and reprisal"); to raise and support the army and navy; to prescribe "Rules for the Government and Regulation of the land and naval Forces"; to define offenses against the law of nations; and to spend federal dollars.[62] In addition, Congress has expansive authority to "make all Laws which shall be necessary and proper for carrying into Execution ... all ... Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."[63] The President, meanwhile, is constitutionally obligated to "take Care that the Laws be faithfully executed,"[64] including FISA. The "Commander in Chief" role is not even described as a "power," and is plainly subject to the legislative powers assigned to Congress by Article I. These constitutional provisions make clear that while the framers recognized the necessity and desirability of giving the President the authority to direct the troops, it also recognized the real dangers of Presidential wartime authority—and sought very explicitly to limit that authority by vesting in Congress broad authority to create, fund, and regulate the very forces that engage the enemy. These textual provisions cannot be read to afford the President uncheckable authority to choose the "means and methods of engaging the enemy."

History also supports this conclusion. Congress has routinely enacted statutes regulating the Commander in Chief's "means and methods of engaging the enemy." It has subjected the Armed Forces to the Uniform Code of Military Justice, 10 U.S.C. §§ 801-946, which expressly restricts the means the President may employ in "engaging the enemy." It has enacted statutes

---

62 U.S. Const., art. I, § 8, cls. 11; 12 & 13; 14; 10; and 1, respectively.
63 U.S. Const., art. I, § 8, cl. 18.
64 U.S. Const., art. II, § 3.

setting forth the rules for governing occupied territory, and these statutes displace Presidential regulations governing such "enemy territory" in the absence of legislation. *See Santiago v. Nogueras*, 214 U.S. 260, 265-66 (1909). And most recently, it has enacted statutes prohibiting torture under all circumstances, 18 U.S.C. §§ 2340-2340A, and prohibiting the use of cruel, inhuman, and degrading treatment by U.S. officials and military personnel anywhere in the world. Pub. L. No. 109-148, Div. A, tit. X, § 1003, 119 Stat. 2739-40 (2005).

If defendants were correct that Congress cannot interfere with the Commander in Chief's discretion in "engaging the enemy," all of these statutes would be unconstitutional. Yet President Bush has conceded that he may not order torture as Commander in Chief.[65] Torturing a suspect, no less than wiretapping an American, might provide information about the enemy that could conceivably help prevent a future attack, yet President Bush has conceded that Congress can prohibit that conduct. Congress has as much authority to regulate wiretapping of Americans as it has to regulate torture and inhuman treatment of foreign detainees.[66] Accordingly, the President cannot simply contravene Congress's clear criminal prohibitions on electronic surveillance.

B. FISA Does Not Impermissibly Interfere with the President's Role as Commander in Chief

The Justice Department has also argued that even if Congress may regulate "signals intelligence" during wartime to some degree, if FISA precludes warrantless wiretapping of

---

[65] In an interview on CBS News, President Bush said "I don't think a President can order torture, for example…. There are clear red lines." Eric Lichtblau & Adam Liptak, *Bush and His Senior Aides Press On in Legal Defense for Wiretapping Program*, N.Y. Times, Jan. 28, 2006, at A13.

[66] The DOJ Memo oddly suggests that Congress's authority to enact FISA is less "clear" than was the power of Congress to act in *Youngstown* and *Little v. Barreme*, both of which involved congressional action at what the DOJ calls the "core" of Congress's enumerated Article I powers—regulating commerce. DOJ Memo at 33. But FISA was also enacted pursuant to "core" Article I powers—including the same foreign commerce power at issue in *Little*, and, as applied to the NSA, Congress's powers under the Rules for Government and Necessary and Proper Clauses.

Americans in the context of the NSA spying program it impermissibly intrudes on the President's exercise of his Commander in Chief role.[67] In fact, FISA's regulation is quite limited, and expressly permits wiretapping of foreign agents, including members of international terrorist organizations, merely requiring judicial confirmation that there is a factual basis for doing so.

It is important to note first that FISA is triggered only when surveillance is "targeting [a] United States person who is in the United States," or the surveillance "acquisition occurs in the United States."[68] FISA does not regulate electronic surveillance acquired abroad and targeted at non-U.S. persons. Thus, it does not limit in any respect wholly foreign surveillance of al Qaeda, or indeed even of all persons in Afghanistan.

Second, even when the target of surveillance is a U.S. person within the United States, or the information is physically acquired here, FISA permits wiretaps, but merely requires that they be approved by a judge, based on a showing of probable cause that the target is an "agent of a foreign power," which includes a member of a terrorist organization.[69] Such judicial approval may be obtained *after* the wiretap is put in place, so long as it is sought within 72 hours.[70]

Because FISA leaves unregulated electronic surveillance conducted outside the United States and not targeted at U.S. persons, it leaves to the President's unfettered discretion a wide swath of "signals intelligence." Moreover, it does not actually prohibit *any* signals intelligence regarding al Qaeda, but merely requires judicial approval where the surveillance targets a U.S. person or is acquired here. As such, the statute cannot reasonably be said to intrude impermissibly upon the President's ability to "engage the enemy," and certainly does not come

---

67 DOJ Memo at 29, 34-35.

68 50 U.S.C. § 1801(f)(1)-(2).

69 *See id.* §§ 1801(a)-(b), 1805(a)-(b). If the target is a non-U.S. person, it is sufficient to show that he is a "lone wolf" terrorist. *Id.*

70 *Id.* § 1805(f).

anywhere close to "prohibit[ing] the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack," as the Justice Department has asserted.[71]

In support of its constitutional argument, the Justice Department has invoked the decision of the Foreign Intelligence Surveillance Court in *In re Sealed Case No. 02-001*.[72] The court in that case did assume, in dictum, that the President has some inherent authority to gather foreign intelligence, and that Congress cannot "encroach on the President's constitutional power." 310 F.3d at 742. But this statement is a truism. The court plainly did not mean that *any regulation* of foreign intelligence gathering amounts to impermissible "encroachment," because it upheld FISA in that very case (as has every court to consider it since its enactment in 1978). Indeed, the court did not even attempt to define what sorts of regulations would constitute impermissible "encroachment."

In addition, the only decision cited in *In re Sealed Case* for the proposition that the President has inherent authority to engage in certain foreign intelligence surveillance addressed the President's power *before FISA was enacted*. *See In re Sealed Case*, 310 F.3d at 742 (*citing United States v. Truong Dinh Hung*, 629 F.2d 908, 915 n.4 (4th Cir. 1980)). The *Truong* decision, which came down after FISA was enacted but reviewed the constitutionality of pre-FISA surveillance, also acknowledged that FISA itself was constitutional, so did not suggest that the President's "inherent" power was in any way immune from congressional regulation. *Truong Dinh Hung*, 629 F.2d at 915 n.4.

In fact, all the cases that have recognized inherent Presidential authority to conduct foreign intelligence surveillance have addressed the President's pre-FISA authority. But the

---

71 DOJ Memo at 35.

72 310 F.3d 717, 742 (For. Intell. Surveillance Ct. Rev. 2002) (per curiam).

President's authority before FISA was enacted was radically different from his authority after FISA. Before FISA was enacted, Congress had left open the question of whether the President has "constitutional power … to obtain foreign intelligence information deemed essential to the security of the United States." 18 U.S.C. § 2511(3) (1968).[73] Before FISA, the President was acting "in the absence of either a Congressional grant or denial of authority," Justice Jackson's "category two," the "zone of twilight" in which the President and Congress "may have concurrent authority, or in which [the] distribution [of power] is uncertain." *Youngstown*, 343 U.S. at 637 (Jackson, J. concurring).

When Congress enacted FISA in the wake of demonstrated abuses of that power, however, it repealed the provision approving of inherent presidential foreign intelligence gathering, and made it a crime to conduct wiretapping without congressional authority. In authorizing the NSA to conduct warrantless wiretapping in contravention of FISA's criminal prohibition, the President is therefore acting in Justice Jackson's "category three." There, the President's power is at its "lowest ebb." Thus, the fact that some lower federal courts may have ruled that the President may have had the power to act when Congress had been silent with respect to his power does not mean that the President can choose to violate a duly enacted criminal prohibition after Congress has "acted upon the subject." *Id*. at 638-39.

Some statutes might well impermissibly interfere with the President's role as Commander in Chief. If Congress sought to place authority to direct battlefield operations in an officer not subject to the President's supervision, for example, such a statute might well violate the

---

[73] The Government argued in *Keith* that this provision in Title III amounted to recognition by Congress that the President had authority to conduct electronic surveillance in national security cases without judicial approval. The Supreme Court flatly rejected this contention and concluded that the section conferred no power on the President, but merely meant that Congress was not legislating in Title III with respect to national security surveillances. *Keith,* 407 U.S. at 303–08. The Court held that Title III left the President only with such power as the Constitution might confer with respect to national security surveillance and neither expanded nor contracted such power.

President's role as Commander in Chief. Similarly, Congress should not be constitutionally permitted to micromanage tactical decisions in particular battles. But short of such highly unlikely hypotheticals, Congress has broad leeway to govern and regulate the armed services, to define the scope of a military conflict, to fund only the weapons and programs it approves, and certainly to protect the privacy expectations of Americans using telephone and email communications.

IV. The NSA Spying Program Violates the First and Fourth Amendments

The NSA program also violates the First and Fourth Amendments. It intrudes directly on constitutionally protected speech, and invades plaintiffs' reasonable expectation of privacy in their telephone and email communications with clients and others overseas. The existence of the program, and its targeting at some of their clients, has chilled plaintiffs' exercise of First Amendment rights, and burdened their ability to seek judicial redress on behalf of their clients.

A. The Program Violates the Fourth Amendment Because It Permits Highly Intrusive Invasions of Privacy without a Warrant or Probable Cause.

The Fourth Amendment imposes an independent limit on the power of the government to engage in electronic surveillance without a judicial warrant. Even if the AUMF could be read as Congressional authorization to engage in warrantless electronic surveillance, the Fourth Amendment would not permit it.[74] No theory of implied executive power asserts that the President can take actions that are proscribed by explicit provisions of the constitution.

[74] Plaintiffs are aware of news reports that some Senators have discussed legislation that would amend FISA to permit electronic surveillance without a warrant. We cannot speculate about what form any such legislation might take, or whether it will be passed by Congress. We do, however, underscore that the First and Fourth Amendments set limits on government power, whether authorized by Congress or not.

As the Supreme Court recognized in *United States v. United States District Court (Keith)*, 407 U.S. 297, 313-14 (1972), private, confidential communications are protected by the Fourth Amendment, and are essential to the exercise of First Amendment freedoms of speech, association, and petition. The warrant and probable cause requirements thus serve to protect both privacy and speech interests. And it is precisely in national security cases that First and Fourth Amendment rights are most likely to be imperiled:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. … History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. [75]

Keith held that probable cause and a warrant were required for electronic surveillance authorized by the Attorney General, on behalf of the President, of domestic persons who allegedly constituted a threat to the national security. Although the *Keith* Court recognized that there are exceptions to the warrant requirement, "few in number and carefully delineated," 407 U.S. at 318 (citing *Katz v. United States*, 389 U.S. at 357), it refused to accept the government's argument that the circumstances of domestic security surveillances constituted grounds to establish a new exception for such cases. The Court specifically rejected the government's arguments that requiring prior judicial review would obstruct the President in the exercise of his duty to protect national security; that such surveillance was exempt from the Fourth Amendment

[75] *Keith*, 407 U.S. at 313-14.

because it was directed primarily to collecting and maintaining intelligence with respect to subversive forces and not for criminal prosecutions; that the warrant requirement was not intended to restrain ongoing intelligence gathering as compared to criminal investigations; that courts would not have sufficiently sophisticated knowledge or techniques to assess whether such surveillance was necessary to protect national security; and that disclosures to judicial officers would compromise the security of informants and agents and the secrecy necessary for intelligence gathering. 407 U.S. at 318-20.

The *Keith* Court did not directly address whether the Constitution forbids warrantless electronic surveillance of foreign powers or their agents in national security cases. But its reasoning nonetheless strongly supports the conclusion that a warrant is required for electronic surveillance of foreign agents as well. Protection of the Fourth Amendment rights of all persons within the United States is better served by requiring a warrant before such surveillance is undertaken. And given the 28-year history of FISA, the government cannot show that "a warrant requirement would unduly frustrate the efforts of Government to protect itself." *Keith*, 407 U.S. at 315. Congress has established a special court to hear warrant requests in the national security area, set the standard for issuing such warrants substantially lower than for Title III warrants in ordinary criminal cases, and permitted the President to initiate such electronic surveillance without a warrant in hand in emergency situations. It cannot be argued, therefore, that the warrant requirement unduly frustrates the government's efforts to protect the United States.

The requirement that a neutral, disinterested magistrate be involved in the process of instituting surveillance reflects the basic constitutional premise that executive officers cannot be trusted to police themselves where the privacy rights of individuals are concerned. *McDonald v. United States*, 335 U.S. 451, 455-56 (1948) ("The right of privacy was deemed too precious to

entrust to the discretion of those whose job is the detection of crime.... Power is a heady thing; and history shows that the police acting on their own cannot be trusted."); *Katz*, 389 U.S. at 358-59 ("[B]ypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police.'") (citation and internal quotation marks omitted); *Keith*, 497 U.S. at 317 ("The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised.").

The "indiscriminate wiretapping and bugging of law-abiding citizens" that the *Keith* Court rightly feared are no less likely simply because the targets of such surveillance are suspected of being affiliated with a foreign power.[76] In fact, in the absence of judicial oversight,

---

[76] In the wake of *Keith*, but before the passage of FISA, a handful of cases recognized a foreign intelligence exception to the warrant requirement. *See United States v. Truong*, 629 F.2d 908, 912-15 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875-76 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 604-05 (3d Cir. 1974) (en banc); *United States v. Clay*, 430 F.2d 165, 170-71 (5th Cir. 1970). These cases do not apply in this Circuit, are inconsistent with the Supreme Court's rationale in *Keith*, and their rationale—that judges are incompetent to deal with intelligence matters, and that delays and leaks would threaten national security—has now been undermined by over twenty-five years of experience under FISA. Indeed, FISA contains provisions for emergency FISA orders, there is no history of leaks under FISA, and FISA judges have had no difficulty understanding the "delicate and complex decisions that lie behind foreign intelligence surveillance," *Truong*, 629 F.2d at 913, well enough to grant the executive nearly all the warrants it claimed to need.

Moreover, not all of the Circuits that ruled on the issue before FISA came to the same conclusion: four of eight judges on the en banc D.C. Circuit agreed (albeit in dicta) that "absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." *Zweibon v. Mitchell*, 516 F.2d 594, 614 (D.C. Cir. 1975) (en banc) (plurality opinion). After an exhaustive discussion of the implications of the *Keith* decision, the plurality's analysis highlighted an ominous implication of recognizing a foreign intelligence exception to the warrant requirement: there is no principled basis upon which to confine such an exception to electronic surveillance alone. If the President's foreign affairs authority and the supposed incompetence of the judiciary are strong enough reasons to abrogate long-established protections of Americans' private telephone calls in the name of national security, on what basis could courts step in and prevent executive officers from "rummag[ing] through the books, papers, and other effects of dissidents in the United States based on an Executive determination that they posed a threat to national security"? *Id.* at 618 n.67. Attorney General Gonzales, when pressed on this point before the Senate Judiciary Committee, refused to rule out the possibility that the present administration has engaged in warrantless physical searches of homes or offices in pursuit of its national security policies. *See Wartime Executive Power and the NSA's Surveillance Authority Before the Senate Judiciary Committee*, 109th Congress (Feb. 6, 2006) (SENATOR SCHUMER: "Has the government searched someone's home, an American citizen, or office, without a warrant since 9/11, let's say?" / ALBERTO GONZALES: "To my knowledge, that has not happened under the terrorist surveillance program, and I'm not going to go beyond that.").

The *Zweibon* plurality wisely counseled avoidance of that conundrum: "Given the fact that warrantless trespassory searches were the "hard core" Executive abuses which the Fourth Amendment was designed to proscribe, and the fact that *Katz* abrogated the trespassory/non-trespassory line as a viable criterion for categorizing Executive actions for Fourth Amendment purposes, we believe it is more in keeping with the spirit and purpose of the Fourth Amendment to close areas of assertedly nonreviewable Executive prerogative rather than to retreat in

no one can be sure that surveillance targets are in fact affiliated with a foreign power (or fit the far vaguer standard of the NSA Program).

There is no reason that the executive's institutional tendency to undervalue privacy and err on the side of intrusions should be diminished where the targets of the investigation are suspected of being foreign agents; if anything, executive officers can be expected to err in favor of surveillance even more markedly when investigating threats they believe to be foreign, because the officers may not believe Americans' rights are at stake. Relying on NSA shift supervisors to safeguard the privacy rights of Americans would resurrect the precise evil against which the Fourth Amendment was directed, by "plac[ing] the liberty of every man in the hands of every petty officer." *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (quoting James Otis's description of the British writs of assistance, as discussed in *Boyd v. United States*, 116 U.S. 616, 625 (1886)) (internal quotation marks omitted). A system of warrantless searches authorized in secret by an unaccountable and anonymous officer for a vague purpose with no review by a disinterested magistrate simply cannot qualify as "reasonable" under the Fourth Amendment.

The only rationale advanced by the administration for squaring its program with the Fourth Amendment is unpersuasive. The Justice Department contends that the NSA program can be justified under a line of Fourth Amendment cases permitting searches without warrants and probable cause in order to further "special needs" above and beyond ordinary law enforcement.[77] The Supreme Court has recognized, however, that "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its

---

doctrinal areas which have been settled since the Amendment was first promulgated." 516 F.2d at 618 n.67 (citation omitted).

[77] DOJ Memo at 36-41.

balancing of interests for that of the Framers."[78] The fact that FISA has been used successfully for almost thirty years demonstrates that a warrant and probable cause regime is *not* impracticable for foreign intelligence surveillance.

The Court has used the "special needs" doctrine to uphold highway drunk driving checkpoints, finding them reasonable because they are standardized, the stops are very brief and only minimally intrusive, and a warrant and probable cause requirement would defeat the purpose of keeping drunk drivers off the road.[79] Similarly, the Court has upheld school drug testing programs under the "special needs" doctrine, finding them reasonable because students have diminished expectations of privacy in school, the programs are limited to students engaging in extracurricular programs (so students have advance notice and the choice to opt out), and the drug testing is standardized and tests only for the presence of drugs.[80]

The NSA spying program has *none* of the safeguards found critical to upholding "special needs" searches in these contexts. All the special needs cases contain certain elements: impracticability of the warrant or probable cause requirement; standardized testing or notice and/or an opportunity not to participate in the test-invoking activity; and most significantly, a minimal intrusion on privacy because the search takes place in a setting where expectations of privacy are reduced (because it involves either students in a secondary school, voluntary participation in certain activities, probation, a high security and highly regulated job, or consent[81]). Unlike a minimally intrusive brief stop on a highway or a urine test, the NSA

---

78 *New Jersey v. T.L.O.,* 469 U.S. 325, 352 (1985).

79 *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990).

80 *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646 (1995).

81 *See New Jersey v. T.L.O.*, 469 U.S. 325 (1985) (students in secondary school); *Vernonia School District v. Action*, 515 U.S. 646 (1995) (voluntary participation in certain activities); *Board of Education v. Earls*, 536 U.S. 822 (2002) (same); *Griffin v. Wisconsin*, 483 U.S 868 (1987) (probation); *United States v. Knights*, 534 U.S. 112 (2001) (same); *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989) (high security and highly regulated job); *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602 (1989) (same); *United States v. Knights*, 534 U.S. 112 (2001) (consent).

program consists of wiretapping private telephone and email communications—searches of a sort the Supreme Court has found to be among the most intrusive available to the government.[82] The Program is not standardized, but subject to discretionary targeting under a standard and process that remain secret. Those whose privacy is intruded upon have no notice or choice to opt out of the surveillance. And it is neither limited to the environment of a school nor analogous to a brief stop for a few seconds at a highway checkpoint.

Accordingly, to extend the "special needs" doctrine to the NSA program, which authorizes unlimited warrantless wiretapping of the most private of conversations without statutory authority, judicial review, or probable cause, would be to render that doctrine unrecognizable. It would require all Americans who communicate internationally to have a diminished expectation of privacy, comparable to that of school children, probationers, and employees in heavily regulated environments.

---

[82] Electronic eavesdropping "[b]y its very nature ... involves an intrusion on privacy that is broad in scope," *Berger v. New York*, 388 U.S. 41, 56 (1967), and thus bears a dangerous "similarity ... to the general warrants out of which our revolution sprang." *Id*. at 64 (Douglas, J., concurring). Indeed, "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Id.* at 63 (Douglas, J., concurring). Unlike physical search warrants allowing for "one limited intrusion," the *Berger* court found that the New York wiretapping statute at issue allowed "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." *Id*. at 59 (opinion of the court). Any number of conversations might be seized, "over a prolonged and extended period," *id*. at 57, with any number of parties eavesdropped upon even if only one is the "target" of the surveillance. The statute allowed "no termination date on the eavesdrop once the conversation sought is seized." *Id*. at 59-60. And "because [wiretapping's] success depends on secrecy, [the statute had] no requirement for notice" of a wiretap order. *Id*. at 60.

For all these reasons the *Berger* Court implied that lawful electronic surveillance orders would have to adhere to judicially-supervised safeguards to minimize the impact of the surveillance on privacy—including limits on duration of the surveillance, and some form of showing that no other, less-intrusive means were available that might allow law enforcement to acquire the same information. *Id*. ("a showing of exigency, in order to avoid notice, would appear more important in eavesdropping"). Congress recognized the constitutional dimension of these minimization requirements in both Title III and FISA. *See, e.g*., 50 U.S.C. §§ 1804(a)(5), 1805(a)(4) (mandating that applications and orders under FISA spell out minimization procedures).

B. The Program Violates the First Amendment Because It Authorizes the Interception of Private Communications That Are Fully Protected by the First Amendment without Judicial Safeguards and without Satisfying First Amendment's Substantive Limitations

The NSA program also violates the First Amendment, both because it permits interference with protected political expression without any judicial safeguards, and because it fails to satisfy the substantive requirements of close tailoring that sensitive First Amendment rights demand. The First Amendment also imposes an independent limit on the power of the government to engage in the surveillance challenged here, whether or not such surveillance were to be authorized by Congress.

The Supreme Court has long recognized that the Fourth Amendment protection against unrestricted searches and the First Amendment guarantee of freedom of expression are closely linked. The Bill of Rights "was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961); *see also Stanford v. Texas*, 379 U.S. 476, 485 (1965) (observing that the First, Fourth and Fifth Amendments are "closely related, safeguarding not only privacy and protection against self-incrimination but conscience and human dignity and freedom of expression as well" (citation and internal quotation marks omitted)); *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) ("the struggle from which the Fourth Amendment emerged 'is largely a history of conflict between the Crown and the press'" (quoting *Stanford*, 379 U.S. at 482). Because of the convergence of First and Fourth Amendment values, courts have considered the First Amendment implications of government power to investigate expressive activity when determining whether the exercise of such power complies with the Fourth Amendment. *See, e.g.*, *Zurcher*, 436 U.S. at 564 (requirements of the Fourth

Amendment must be applied with "scrupulous exactitude" where First Amendment rights implicated); *Keith*, 407 U.S. at 313.

The NSA program intrudes on plaintiffs' First Amendment interests by interfering with their ability to communicate with their clients, witnesses, fellow counsel and other persons essential to their work, thereby undermining their First Amendment right to pursue litigation challenging allegedly illegal government programs. The Supreme Court recognized this interest in connection with NAACP advocacy in the civil rights movement:

> the First Amendment … protects vigorous advocacy, certainly of lawful ends, against governmental intrusion. ... In the context of NAACP objectives, litigation is not a technique of resolving private differences; it is a means for achieving the lawful objectives of equality of treatment by all government, federal, state and local, for the members of the Negro community in this country. It is thus a form of political expression.

NAACP v. Button, 371 U.S. 415, 429 (1963). What was true of the NAACP in the 1960's is certainly true of CCR today. The NSA program intrudes upon plaintiffs' right to "petition for redress of grievances," *id*. at 430, and on their "political expression."

The First Amendment imposes both procedural and substantive limits on the NSA spying program. As a procedural matter, the First Amendment strongly underscores the necessity for a judicial court order before presumptively protected speech and associational rights are interfered with. As the Supreme Court has stated in the prior restraint context, "only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression."[83] While an adversarial proceeding is not possible here, at a minimum the First Amendment demands that a judge, *not* an NSA shift supervisor, decide whether the executive branch may compel the disclosure of protected speech. In *Marcus*, the Supreme Court held that a warrant for seizing allegedly obscene material could not issue on the mere conclusory allegations

[83] *Freedman v. Maryland*, 380 U.S. 51, 58 (1965) (requirement of prior submission of film to censor held an invalid prior restraint).

of an executive officer. *Marcus*, 367 U.S. at 724; *see also Lee Art Theatre, Inc. v. Virginia*, 392 U.S. 636-37 (1968) ("warrant issued solely upon the conclusory assertions of the police officer without any inquiry by the justice of the peace into the factual basis for the officer's conclusions ... fell short of constitutional requirements demanding necessary sensitivity to freedom of expression."). "If, as *Marcus* and *Lee Art Theatre* held, a warrant for seizing allegedly obscene material may not issue on the mere conclusory allegations of an officer, *a fortiori*, the officer may not make such a seizure with no warrant at all." *Roaden v. Kentucky,* 413 U.S. 496, 506 (1973). The NSA Program does not provide for any judicial check on electronic surveillance of plaintiffs' protected speech, and for that reason it violates the First Amendment as well as the Fourth Amendment.

The First Amendment also imposes substantive limitations on the extent to which the government may intrude upon protected speech and association. It is well-established, for example, that states may not compel the disclosure of confidential information about a political association absent a compelling interest, a substantial relation between the disclosure required and that interest, and a determination that the request for information is not unduly broad. As the Court of Appeals for the Second Circuit has described it in a case involving a subpoena to provide information regarding a political organization:

> [Plaintiff] claims that his right to freedom of association under the First Amendment shields him from giving testimony concerning the membership, funding, and organizational structure of the HAMC. The standards to be applied to [Plaintiff's] claim are well established. First, the interests of the state must be "compelling," *Bates v. City of Little Rock*, 361 U.S. 516, 524 (1960), and able to survive "exacting scrutiny," *Buckley v. Valeo*, 424 U.S. 1, 64 (1976) (per curiam), as to whether they are "sufficiently important to outweigh the possibility of infringement." *Id*. at 66. Second, there must be some "substantial relation" between the governmental interest and the information required to be disclosed. *Id*. at 64; *Gibson v. Florida Legislative Committee*, 372 U.S. 539, 546 (1963). Third, "justifiable governmental goals may not be achieved by unduly broad means having an unnecessary impact on protected rights of speech, press, or

> association." *Branzburg v. Hayes*, 408 U.S. 665, 680-81 (1972). Finally, an otherwise justifiable investigation may be curtailed when a showing is made that a particularized harm such as harassment or reprisals may result from the disclosure of associational relationships. *Buckley*, 424 U.S. at 74.

In re Grand Jury Proceedings, 776 F.2d 1099, 1103 (2d Cir. 1985).

Because plaintiffs' activity is entitled to the same protection as the right of political association, and because disclosure of attorney-client communications causes at least as much if not more harm to plaintiffs' First Amendment rights than disclosure of membership lists does to a political organization, the same standards must be satisfied here. Conducting surveillance of persons the government has probable cause to believe are agents of a foreign terrorist organization is a government interest sufficiently compelling to justify some interference with First Amendment rights. The means chosen to serve that interest, however, must be narrowly tailored to survive strict scrutiny. The NSA program's broad criteria, as described by the Attorney General, which are not limited to Al Qaeda members, are not narrowly tailored. Moreover, Fourth Amendment standards, or at a minimum FISA's statutory provisions, illustrate narrow tailoring in this context. They identify whose conversations can be overheard and they require judicial involvement in authorizing surveillance. Given FISA's 28-year history, the handful of occasions on which a FISA warrant has been denied over that period,[84] and the emergency provision that permits surveillance to begin 72 hours before a warrant is obtained, the government cannot establish that surveillance through the existing FISA process would not be sufficient to protect the government's legitimate interest.

---

[84] Justice Department statistics indicate that, between 1978 and 2004, the government submitted almost 19,000 surveillance applications to the FISA Court. *See* FISA Annual Reports to Congress 1979-2004, available at http://www.fas.org/irp/agency/doj/fisa/#rept. The Foreign Intelligence Surveillance Court denied four of these applications; granted approximately 180 applications with modifications; and granted the remaining 18,451 without modifications. The number of applications made by the Justice Department and approved by the FISA Court has dramatically increased since 2001. *See id.*

V. CONCLUSION

Plaintiffs request the Court to enter summary judgment[85] in their favor and to issue an injunction prohibiting the defendants from engaging in electronic surveillance without judicial authorization pursuant to the provisions of FISA, as currently enacted, or Title III. This result is required by principles of separation of powers that are the bedrock of our constitutional system, and by the First and Fourth Amendments to the Constitution.

Over the course of American history, presidents have periodically asserted the right to take unilateral action, based on claims that national security demanded it, and have overreached in doing so, violating basic constitutional rights. History has always rendered a judgment that a terrible mistake was made. We have learned that executive overreaching often has posed a risk as great or greater to our democratic way of life than the dangers such officials warned against.

President Bush has not made—and cannot make—a case that there are exigencies that require him to act as he has without the consent of both of the other two branches of government. The rule of law requires that the President be ordered to desist from exercising power that is not authorized by the Constitution and has not been authorized by Congress, and that the President be enjoined from conducting electronic searches without the approval of judicial officers.

Respectfully submitted,

s/Shayana Kadidal
William Goodman [WG-1241]
Shayana Kadidal [SK-1278]
Michael Ratner [MR-3357]
CENTER FOR CONSTITUTIONAL RIGHTS

[85] Plaintiffs seek partial summary judgment based on what the defendants have admitted about the NSA spying program thus far. Plaintiffs reserve the right to seek further relief in light of any further disclosures that are made, through discovery or otherwise, regarding the NSA program.

666 Broadway, 7th Floor
New York, NY 10012-2317
(212) 614-6427

CCR Cooperating Counsel:
David Cole
c/o Georgetown University Law Center
600 New Jersey Avenue, N.W.
Washington, DC 20001
(202) 662-9078

Michael Avery
J. Ashlee Albies
NATIONAL LAWYERS GUILD
c/o Suffolk Law School
120 Tremont Street
Boston, MA 02108
(617) 573-8551

counsel for Plaintiffs

Certificate of Service

I, Shayana Kadidal, certify that on March 9, 2006, I caused the foregoing Memorandum, together with the Notice of Motion, Statement of Undisputed Facts, and the Affirmation of William Goodman (together with its attached exhibits) to be filed electronically on the ECF system and served via email on the counsel for defendants listed below.

Anthony J. Coppolino
Special Litigation Counsel
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, D.C. 20044
Email: *tony.coppolino@usdoj.gov*

Dated: March 9, 2006

s/ Shayana Kadidal
Shayana Kadidal [SK-1278]
CENTER FOR CONSTITUTIONAL RIGHTS
666 Broadway, 7th Floor
New York, NY 10012-2317