Testimony of

Professor Harold Hongju Koh

Dean
Yale Law School
February 28, 2006

Statement of Harold Hongju Koh
Dean and Gerard C. & Bernice Latrobe Smith Professor of International Law
Yale Law School
before the Senate Judiciary Committee
regarding
Wartime Executive Power and the National Security Agency's Surveillance Authority
February 28, 2006

Thank you, Mr. Chairman and Members of the Committee, for inviting me today.

I am Dean and Gerard C. & Bernice Latrobe Smith Professor of International Law at the Yale Law School, where I have taught since 1985 in the areas of international law, human rights, and the law of U.S. foreign relations.1 I appear first, to testify regarding the claimed legal authority for the Administration's National Security Agency (NSA) domestic surveillance program; second, to respond to the Administration's legal defense of the program, as set forth in several recent Justice Department documents and in the Attorney General's testimony before this Committee on February 6, 2006;2 and third, to comment on a draft bill entitled the "National Security Surveillance Act," which I received from this Committee's staff on February 24, 2006.

To state my conclusions briefly: I have served the United States government in both Republican and Democratic Administrations.3 I have also filed lawsuits against both Republican and Democratic administrations when I became convinced that their conduct violated the law.4 In my professional opinion, the ongoing NSA domestic surveillance program is blatantly illegal, whether or not -as its defenders claim--it is limited to international calls with one end in the United States.5

None of the program's defenders - including those who appear today-- has identified any convincing legal justification for conducting such a sweeping program without the legally required checks of congressional authorization and oversight and judicial review. My government service makes me fully sensitive to the ongoing threat from Al Qaeda and the need for law enforcement officials to be able to gather vital information before another terrorist attack occurs. Of course, in time of war, our Constitution recognizes the President as Commander-in-Chief. But the same Constitution requires that the Commander-in-Chief obey the Fourth Amendment, which guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."6 By so saying, the Fourth Amendment requires that any government surveillance be reasonable, supported except in emergency situations by warrants issued by courts, and based upon specific probable cause. The current NSA surveillance program, as I understand it, violates all three constitutional standards.

For nearly thirty years, the Foreign Intelligence Surveillance Act of 1978 (FISA)7 has guaranteed compliance with these constitutional requirements by providing a comprehensive, exclusive statutory framework for electronic surveillance. Even as Commander-in-Chief, the President carries the solemn constitutional duty to "take Care that the Laws be faithfully executed."8 Yet apparently, the NSA has violated these statutory requirements repeatedly by carrying on a sustained program of secret, unreviewed, warrantless electronic surveillance of American citizens and residents. As Justice Paterson wrote two centuries ago in United States v. Smith: "[t]he president of the United States

cannot control the statute, nor dispense with its execution, and still less can he authorize a person to do what law forbids."9

The NSA program's defenders cannot plausibly claim that the ongoing program follows the letter of the FISA. Instead, to justify this flouting of the FISA, they argue both that Congress authorized this program in the resolution authorizing force and offer a sweeping interpretation of unchecked Executive authority that cannot be squared with the vision of shared national security powers evident in our Constitution's text, structure and purpose. That vision of unchecked executive discretion would upset what Justice Robert Jackson in his famous concurrence in the Steel Seizure Case termed the "equilibrium established by our constitutional system."10 Taken seriously, the President's reading of the Constitution would render Congress a pointless rubberstamp, limited in an unending war on terror to enacting laws that the President can ignore at will and issuing blank checks that the President can redefine at will.

Of course, we can and should aggressively fight terrorism, but doing so outside the law is deeply counterproductive.11 The NSA program undermines, rather than enhances, our ability to combat terrorism through the criminal justice system. Under the ongoing NSA program, NSA analysts are increasingly caught between following superior orders and carrying out illegal electronic surveillance. The nation can scarcely afford to lose analysts that are on the front lines protecting our national security. Furthermore, because evidence collected under the NSA electronic surveillance program will almost surely be challenged as illegally obtained, such evidence may prove inadmissible in cases against alleged terrorists, giving them greater leverage in plea bargains and making it far more difficult to prosecute them criminally.

Unfortunately, for reasons detailed below, the proposed National Security Surveillance Act (NSSA) would not improve the situation. Instead of subjecting the legality of the ongoing program to meaningful congressional oversight and contemporaneous judicial review, the proposed law would simply amend the 1978 Foreign Intelligence Surveillance Act to increase the authority of the President to conduct surveillance, based on a showing of "probable cause" that the entire surveillance program -- not any particular act of surveillance -- will intercept communications of a foreign power or agent thereof, or anyone who has ever communicated with a foreign agent. While perhaps legalizing a small number of reasonable searches and seizures, the proposed statute would make matters far worse, by giving the Congress' blanket pre-authorization to a large number of unreasonable searches and seizures. To enact the draft legislation, which ratifies an illegal ongoing program without demanding first a full congressional review of what is now being done and more executive accountability going forward, would provide neither the congressional oversight nor the judicial review that this program needs to restore our confidence in our constitutional checks and balances. Most fundamentally, unless the President agrees to operate within the terms of any FISA amendments, the new congressional action would be meaningless.

I. The Illegality of the Ongoing NSA Domestic Surveillance Program

We must not forget the historical events that led to enactment of the 1978 FISA statute. When American ships were attacked in the Gulf of Tonkin in 1964, President Johnson asked Congress for a broad resolution that gave him broad freedom to conduct a controversial undeclared war in Indochina; that war traumatized our country and triggered a powerful antiwar movement.12 It soon came to light that to support the war effort, three government agencies--the FBI, the CIA, and the NSA - had wiretapped thousands of innocent Americans suspected of committing subversive activities against the U.S. government.13

To end these abuses, Congress passed, and President Carter signed, the Foreign Intelligence Surveillance Act of 1978 (FISA), which makes it a crime for anyone to wiretap Americans in the United States without a warrant or a court order.14 The law makes it clear that the FISA (and specified provisions of the federal criminal code that govern criminal wiretaps) "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire communications may be conducted."15 In an emergency, where the Attorney General believes that surveillance must begin before he can get a court order, FISA permits the wiretap to begin immediately, but only so long as the government seeks a warrant from the special FISA court within 72 hours.16 Drafted with wartime in mind, the FISA permits the Attorney General to authorize warrantless electronic surveillance in the United States for only 15 days after a declaration of war, to give Congress time to pass new laws to give the President any new wiretap authority he may need to deal with the wartime emergency.17 In short, FISA was based on simple, sensible reasoning: before the President invades our privacy, his lawyers must get approval from someone who does not work for him: either

members of Congress must pass an amendment to FISA, or members of the independent Foreign Intelligence Surveillance Court must approve a particular warrant.

For almost thirty years, the FISA scheme worked to protect our rights as American citizens to privacy, while still allowing our government to engage in necessary foreign surveillance. From 1979 to 2004, the FISC approved nearly 19,000 warrants and rejected only five.18 Even since September 11, officials of the Bush Administration officials have obtained thousands of warrants approved by the special FISA court.19 During the last few years, the President was asked several times whether judicial permission is required for any government spying on American citizens; on each occasion, he answered in the affirmative.20 And last January, when Alberto Gonzales was being confirmed as Attorney General, Senator Russ Feingold asked whether he believed the President could violate existing criminal laws and spy on U.S. citizens without a warrant. Mr. Gonzales answered that it was impossible to answer such a "hypothetical question" but that it was "not the policy or the agenda of this president" to authorize actions that conflict with existing law.21

Given this background, as of three months ago, the law seemed crystal clear. If executive officials wanted to wiretap or conduct electronic surveillance of Americans, they could do so without a warrant, but only for three days, or for fifteen days after a declaration of war. After that, they must either go to the special FISA court for an order to approve the surveillance, come to Congress seeking wartime amendments to FISA, or be in violation of the criminal law.

And so we were all stunned to learn in December 2005 that despite this settled law, the Executive Branch has in fact been secretly spying on large numbers of Americans for four years and eavesdropping on "large volumes of telephone calls, e-mail messages, and other Internet traffic inside the United States."22 Despite the clear requirements of the FISA law, the President had apparently launched this eavesdropping program without ever seeking a search warrant. Nor did the Administration ever seek new laws that would authorize such domestic intelligence gathering.23 Moreover, we learned that President Bush has personally authorized this eavesdropping program more than three dozen times since October 2001, at times over the objections of high senior officials in his own Justice Department.24

Although the program's details continue to remain hidden from public view, we now know that intelligence officials apparently persuaded officials of major telecommunications companies to let the NSA monitor communication activity through "electronic backdoors."25 Recent Justice Department documents and statements appear to acknowledge: (1) that the NSA engages in such surveillance without judicial approval, and apparently without the substantive showings that FISA requires--e.g., that the target subject is an "agent of a foreign power;" 26(2) that the NSA determines on its own which phone calls and emails to monitor, without seeking prior approval from the White House, the Justice Department, or any court before it starts monitoring any specific email or phone line; (3) that no lawyer or prosecutor reviews any records before the NSA starts to listen in on a line; 27 and (4) that despite the Administration's assurances, we have no way of knowing that searches will be strictly limited to people who have made contact with Al Qaeda.

Some commentators have claimed that the NSA searching involves only computerized datamining that intercepts little or no communicative content, and hence does not constitute surveillance subject to the FISA or a "search" or "seizure" subject to the Fourth Amendment. But in fact the Attorney General himself has expressly rejected those claims by repeatedly stating that the NSA program involves "electronic surveillance," defined in FISA to mean the interception of the contents of telephone, wire, or e-mail communications that occur, at least in part, in the United States.29 In a press briefing held on December 19, 2005, Attorney General Gonzales also conceded that the NSA program intercepts the "contents of communications"30 and that the "surveillance that . . . the President announced on [December 17]" is the "kind" that "requires a court order before engaging in" it "unless otherwise authorized by statute or by Congress."31

On its face, the NSA Program blatantly violates the statutory FISA standards outlined above. By their own admission, the Administration's officials did not seek a warrant within three days of commencing the NSA Program, nor did they do so within fifteen days after the congressional resolution authorizing the use of force, nor have they done so in the nearly four years since. To this day, the Administration has yet to offer any convincing explanation why it could not have sought or obtained warrants from the special FISA court created for this purpose, which has approved tens of thousands of warrants over the years. Nor despite the many post hoc legal justifications that have been released

since December, has the Administration yet to make public any contemporaneous legal opinion provided to the President upon which its decision to launch the NSA program was actually based.32

When the President acts in a field in which Congress has legislated so comprehensively, the acknowledged touchstone for constitutional analysis is Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure Case), in which the Supreme Court invalidated an attempted presidential takeover of the steel mills in the name of national security during the Korean War.33 In his landmark concurring opinion in that case, Justice Robert Jackson wrote: "Presidential powers are not fixed, but fluctuate, depending on their ... disjunction with those of Congress. When the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only on his own constitutional powers minus any constitutional powers of Congress over the matter."34

The FISA was enacted by Congress precisely to regulate the kind of surveillance that has occurred here. In response, the Justice Department asserts that the President may choose clandestinely to ignore the FISA. Youngstown thus requires us to ask whether the Constitution subjects the presidential power at issue in this case to the control of statutes passed by Congress with the assent of the President, or whether the Constitution confides that power exclusively in the President.

The Justice Department claims that the President has an implied exclusive executive authority over "the means and methods of engaging the enemy," including the conduct of "signals intelligence" during wartime.35 Yet nothing in the text of Article II of the Constitution recognizes an exclusive presidential power to conduct warrantless, unreviewed wiretapping, akin to the textual powers to appoint or pardon, to veto legislation, or to recognize foreign governments. Nor is it clear that the Fourth Amendment would allow a sustained program of unchecked warrantless wiretapping within the United States, even if expressly authorized by Congress and President acting together.36

As Justice Jackson wrote in Youngstown, "the Constitution did not contemplate that the title Commander in Chief of the Army and Navy will constitute him also Commander in Chief of the country, its industries and inhabitants."37 Congress undeniably has power "To make Rules for the Government and Regulation of the land and naval Forces" and 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."38 Under these authorities, Congress has enacted myriad statutes regulating the "means and methods of engaging the enemy," including most obviously, the Uniform Code of Military Justice and the recent, much-discussed statutes prohibiting the use of torture and cruel, inhuman, and degrading treatment.39 And whether or not the President as Commander in Chief may generally collect "signals intelligence" on the enemy abroad, no one denies that Congress may regulate electronic surveillance within the United States, as it has expressly done in FISA. Every Supreme Court decision to confront the question has rejected the claim that the President may invoke his Commander in Chief power to disregard an Act of Congress
designed specifically to restrain executive conduct in a particular field.40 If anything, such claim of presidential power deserves even less deference when Fourth Amendment values and a criminal statutory prohibition are at stake.41

In sum, under Youngstown's reasoning, given that "the President [has] take[n] measures incompatible with the express or implied will of Congress" as expressed in FISA, "his power is at its lowest ebb, for then he can rely only on his own constitutional powers minus any constitutional powers of Congress over the matter."42 Whether or not there are historical examples of the President engaging in warrantless wartime surveillance before the FISA was passed, it seems clear that he may not now constitutionally undertake such actions where Congress and the President have not just contemplated such behavior, but actually criminalized it.

II. The Arguments Defending the NSA Program Cannot Withstand Scrutiny

Since the domestic spying program came to light, the Administration has launched a broad public campaign to defend its legality. Let me explain why none of these legal and policy arguments withstand scrutiny.

A. The 2001 Authorization for Use of Military Force (AUMF) Resolution Does Not Authorize Domestic Surveillance

The Administration claims that the Congress implicitly authorized the NSA surveillance plan when it voted for the Authorization to Use Military Force (AUMF) Resolution in September 2001.44 That law authorizes the President to use "all necessary and appropriate force" against "nations, organizations, or persons" associated with the terrorist attacks of September 11, 2001, in order to protect the nation from the recurrence of such attacks. But to read this law as the President's lawyers do would recreate the Gulf of Tonkin Resolution: a law construed after the fact to give him a blank check to engage in broad domestic activities, in this case wiretapping of Americans on U.S. soil without a warrant. To accept that reading, Congress would now have to conclude that in September 2001, it silently approved what 23 years earlier it had expressly criminalized!

Absent "overwhelming evidence" of an "irreconcilable conflict"--neither of which exist here--45 we cannot assume that Congress intended in the AUMF silently to repeal 18 U.S.C. § 2511(2)(f), which makes the FISA (and other specific criminal code provisions) "the exclusive means by which electronic surveillance...may be conducted." When first asked why the Administration had not sought to amend FISA to authorize the NSA spying program, Attorney General Gonzales acknowledged, "[w]e 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." 46 Yet remarkably, after candidly admitting that Congress would not have authorized the spying program, had it known about it, the Attorney General now argues that in fact, Congress silently authorized it four years earlier when it passed the AUMF, although that law nowhere mentions surveillance of any kind.

This argument does not pass the "straight face" test.47 In FISA, Congress not only specified the "exclusive means" for conducting domestic surveillance, but also specifically required that any domestic warrantless wiretapping be limited to fifteen days after a declaration of war.48 "[W]hen Congress did specifically address itself to a problem, as Congress did [here,] to find secreted in the interstices of legislation the very grant of power which Congress consciously withheld...is ...to disrespect the whole legislative process and the constitutional division of authority between President and Congress.49

Remarkably, in his testimony before this Committee, the Attorney General repeatedly invoked Hamdi v. Rumsfeld50--in which the Supreme Court largely rejected the President's arguments--to support his reading of the AUMF. But in Hamdi, a plurality of the Court held only that the AUMF authorized as a "fundamental incident of waging war" the military detention of enemy combatants captured on the battlefield abroad who were "part of or supporting forces hostile to the United States or coalition partners in Afghanistan and who engaged in an armed conflict against the United States there" "for the duration of the particular conflict in which they were captured," in order to prevent them "from returning to the field of battle and taking up arms once again."51 But if, as the Hamdi plurality agreed, the AUMF does not authorize "indefinite detention [even of enemy combatants] for the purpose of interrogation," 52 why read the AUMF to authorize indefinite domestic wiretapping of American citizens who are not alleged to be enemy combatants, for the purpose of information-gathering? Indeed, while the AUMF was being debated, the Administration sought to have language inserted in it that would have authorized the use of military force domestically - which Congress rejected. 53 If the AUMF authorization were actually as broad as the Administration now claims, why should the Administration request and the Congress now bother to reenact the USA PATRIOT Act? No less than the FISA, the various investigative and preventive authorities of the USA PATRIOT Act could already be undertaken by the President unilaterally under the AUMF.

B. We Have No Proof that The NSA Domestic Surveillance Program is Narrowly Aimed Only at Al Qaeda and its Associates.

At the Attorney General's December 19 press briefing, he noted that the four- year-old surveillance program applies narrowly only to "communications, back and forth, from within the United States to overseas with members of Al Qaeda." 54 In fact, there is mounting evidence that NSA has a second program that is a much broader operation that is violating the rights of uncounted innocent Americans.55 The New York Times reported that the NSA swept up thousands of e-mail messages and telephone calls to generate thousands of leads.56 The Washington Post recently reported that about 5000 "Americans in the past four years have had their conversations recorded or their e-mails read by intelligence analysts without court authority." Of those, "[f]ewer than 10 U.S. citizens or residents a year, according to an authoritative account, have aroused enough suspicion during warrantless eavesdropping to justify interception of their domestic calls."57

At the same press briefing, the Attorney General revised his remarks to say that the NSA will eavesdrop whenever "we . . . 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."58 Under this reasoning, the NSA could conduct a secret, indefinite warrantless wiretap of phone calls and emails between two U.S. citizens living in the U.S., so long as one had once worshipped at a mosque that the Administration had concluded is in some way "supportive" of al-Qaeda. Yet in such a case, the total absence of congressional oversight and judicial review would leave those citizens' Fourth Amendment rights to privacy unprotected.59

C. We Have No Reason to Believe The NSA Program Would Have Prevented September 11

Another claim that cannot stand is that the attacks of September 11 could have been prevented if only the NSA Program had been in place. In fact, nothing in our law prevented American intelligence from listening to a call to or from the United States involving Al Qaeda before September 11, so long as they got the warrant duly required by the FISA. Indeed, as the 9/11 Commission Report amply showed, our government already had plenty of evidence before September 11 that attacks would occur. The Commission found that the failure of the government to register the significance of that evidence resulted not from any restriction (in FISA or any other law) on information gathering, but rather from restrictions on information-sharing within the government.60 In short, Administration officials did not miss the 9/11 plot because they took the few hours necessary to get a FISA warrant to eavesdrop on phone calls and e-mail messages. If anything, they missed the plot because existing procedures made them overlook information that was already in the system.

D. Giving Restricted Information to the "Gang of Eight" Did Not Substitute for Genuine Congressional Oversight or Judicial Review

Some have also argued that Congress was "effectively informed" of the NSA Program by classified briefings that were given to the "Gang of Eight," the chair and ranking members of both intelligence committees, the majority and minority leaders of the Senate, and the Speaker and minority leader of the House. But we know from Senator Rockefeller's handwritten - and unanswered - letter to Vice President Cheney of July 17, 2003, and from several others among the Eight, that several of the Members did not find the briefings sufficiently informative to perform their oversight duty; that some protested and had their protests ignored; and that all believed that they were strictly barred from discussing the briefings they were given with the full intelligence committees and committee staff.61

The law regarding intelligence oversight only allows briefings to be restricted to the Gang of Eight in the case of a covert operation in which a formal presidential finding has been issued; no one has said such a finding was issued here62 (and even had the NSA program been designated a covert operation by the President, that would not have cured its illegality under FISA). Failure to brief the full intelligence committees as required by the National Security Act of 1947 denied the Gang of Eight the assistance of committee staff who had the technical and legal expertise to evaluate the program and to prepare a classified portion of an intelligence bill approving, denying funding for, or regulating the program pursuant to the Congress's explicit constitutional power to appropriate funds and to Govern and Regulate the Armed Forces.63 By so limiting the briefing, the Executive effectively demanded that its co-equal branch of government accept a likely illegal program as a fait accompli.

Under the Intelligence Oversight Act, the Gang of Eight is to be used only for covert operations "in extraordinary circumstances affecting vital interests of the United States," not as a general substitute for the case-by-case independent judicial review for individual surveillance warrants based on probable cause required from the Foreign Intelligence Surveillance Court.64 The fact that a few Members have been given limited information about the NSA program does not constitute congressional oversight, much
less congressional approval of the program, and in any event does not substitute for the genuine judicial review required by FISA.65

E. All Other Administrations Since 1978 Have Obeyed the FISA

Finally, the Attorney General argued in his testimony to this Committee that many Presidents --dating back to George Washington, Woodrow Wilson and Franklin D. Roosevelt ---have all conducted various forms of wartime surveillance. Tellingly, he failed to mention the most important President, Richard Nixon, whose Vietnam-era surveillance of

antiwar groups and political opponents led to FISA's enactment in the first place. Under questioning by Senator Feingold, the Attorney General essentially conceded that no other President has openly evaded the FISA after 1978.66 The fact that Presidents historically collected signals intelligence on the enemy during wartime when Congress did not regulate foreign intelligence gathering in no way exempts this President from now following FISA--which expressly requires that the statutory warrant process be followed more than 15 days after a declaration of war.

III. The proposed National Security Surveillance Act Should Not Be Adopted.

I have only had a short time to examine the staff proposal for a "National Security Surveillance Act," (NSSA) but my strong reaction is that its enactment would be entirely premature. It is the main job of this Committee, I believe, to investigate and determine whether the ongoing NSA program has violated the law for the last four years, and if so, to consider possible legislative remedies for those violations. At the same time, all members of the Congressional Intelligence Committees--not just the Gang of Eight--should now be "fully and currently" briefed on all operational details of the President's NSA program, as required by the National Security Act of 1947. If and when those committees have been fully briefed, they should immediately hold legislative hearings, with expert witnesses, to determine whether the ongoing NSA surveillance program can be brought into compliance with the existing FISA law. Only when these two parallel Committee processes -on the Judiciary side and the Intelligence side--have been completed, will the time be ripe for the two Committees to consider legislative proposals to amend the FISA, which was itself the product of several years of commission and committee studies, and extensive legislative hearings under two Presidential Administrations.

To proceed hastily to "quick-fix legislation"--without full investigation, subpoenas answered, legal opinions disclosed, facts fully aired, Members fully briefed and the public fully informed--would inevitably invite bad legislative process. How can Congress meaningfully legislate to repair the illegalities of the ongoing NSA surveillance program when only a tiny percentage of Congress has been briefed on how that program has actually operated? And how can Congress responsibly amend the mandate of the Foreign Intelligence Surveillance Court, when the Administration has made no showing that that court could not have handled the matters that the Executive Branch illegally avoided bringing to it?

The proposed bill would not improve the situation. Instead of subjecting the legality of the ongoing program to meaningful congressional oversight and contemporaneous judicial review, the proposed law would simply amend the 1978 FISA to increase the authority of the President to conduct surveillance based on a showing of "probable cause" that the entire surveillance program -- not any particular act of surveillance -- will intercept communications of a foreign power or agent thereof, or anyone who has ever communicated with a foreign agent.

Under FISA, the federal government may not engage in electronic surveillance targeted at a U.S. citizen or resident absent probable cause that the "target ... is a foreign power or agent of a foreign power.67 But under the proposed bill, the NSA need not show that either party to an intercepted phone call or e-mail has any connection to Al Qaeda or any other terrorist organization. Nor would the government need to show probable cause that either party to a call or e-mail is a foreign power, an agent of a foreign power, or even associated with a foreign power. Instead, the bill would permit domestic electronic surveillance targeted at U.S. persons based solely upon a showing of "probable cause" that the surveillance program as a whole -- not even the particular surveillance - "will intercept communications of the foreign power or agent of a foreign power specified in the application, or a person who has had communication with the foreign power or agent of a foreign power specified in the application."68

On its face, this language is stunningly broad. Almost every American who has ever stood in a visa line or traveled abroad and spoken to a foreign policeman "has had communication with the agent of a foreign power."69 If this bill became law, the NSA could wiretap virtually any U.S. person or resident almost indefinitely,70 without any showing that any of the target's communications have anything to do with Al Qaeda. The FISA court would then certify that the program as a whole (not any particular surveillance) is "consistent with" the Fourth Amendment in a secret, ex parte proceeding. Such wholesale ratification would be hard to square with the Fourth Amendment's requirement that any government surveillance be reasonable, supported by warrants issued by courts, and based upon specific probable cause in each case.

For example, this draft proposal would authorize the FISA Court to issue a general warrant whereby the NSA could conduct a program seizing all voice and e-mail communications traveling through a switch in New York City and sort

through those communications as part of an "electronic surveillance program," the purpose of which is to collect foreign intelligence information concerning the activities of a religious order connected with a foreign power. The NSA would be authorized to sort through all the messages to obtain all those received by anyone who had ever had communications with any individuals who had ever been in contact with that religious order, or with any agent of any other foreign power. The NSA would then be free to listen to all such communications; to disseminate all such communications to any other intelligence agency; to keep all communications seized in its computers forever (whether listened to or not); to use the warrantless intercepts as evidence against the person; or to use the intercepts as a basis for getting a standard FISA warrant against that person.71

In short, the proposed bill would unwisely shift the focus of FISA from people to "programs," and allow entire programs to be authorized based upon a general showing of "consistency" with the Constitution.72 While perhaps legalizing a small number of reasonable searches and seizures, the proposed statute would make matters far worse, by giving Congress' blanket pre-authorization to a large number of unreasonable searches and seizures. The bill would do nothing to correct the blatant illegality of the ongoing program, and would potentially invite more of the same.

IV. Conclusion

The NSA surveillance program is blatantly illegal because it permits wiretapping within the United States without any of the safeguards for electronic surveillance presumptively required by the Fourth Amendment or FISA --statutory authorization, individualized probable cause, or a warrant or other order issued by a judge or magistrate. The Supreme Court has never upheld such a sweeping, unchecked power of government to invade the privacy of Americans without individualized suspicion or congressional or judicial oversight. None of the defenses offered by the Administration explain why it refused to follow the time-tested warrant requirements of the FISA Court. If the Administration felt that FISA was insufficient for its present-day needs, it should have sought a legislative amendment--as Congress expressly contemplated when it enacted the wartime wiretap provision in FISA. Instead, the Administration conducted a covert end-run around FISA, and when that end-run came to light, it claimed incorrectly that its actions were legal.

As Justice Jackson noted, "power to legislate . . . belongs in the hands of Congress, but only Congress itself can prevent power from slipping through its fingers."73 Congress should now investigate, fully inform itself of the facts, and legislate a remedy to this illegal episode. For reasons I have explained, it would be premature and unwise to enact the draft National Security Surveillance Act bill. Convening prompt, full-scale hearings, perhaps in joint session with the Intelligence Committees, would give this body time to consider a number of thoughtful legislative proposals, including those put forward by the ABA's Task Force on Domestic Surveillance.74

In recent months, some have asked why they should care if the NSA illegally monitors domestic emails and phone calls. Why shouldn't the government have a right to rummage through our communications, if it helps them to find information that warns them of terrorist attacks? In response, I ask whether they have heard of the British "general warrant" of the 1700s. Under the general warrant, British authorities could break into any shop or place suspected of containing evidence of potential enemies of the state.75 I remind them that it was precisely because English law did not sufficiently protect the right of personal privacy that our ancestors in the new American colonies forbade general warrants and demanded specific warrants. Even while recognizing the President as our Commander in Chief, they adopted a Fourth Amendment to the Constitution that ensured that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, ...particularly describing the place to be searched, and the persons or things to be seized."

As a former government official and law dean, I oppose the domestice spying program because it violates our right, as the people, to be secure against unreasonable searches and seizures. The fact some of the many searches now ongoing might be reasonable responses to terrorism cannot justify the uncounted unreasonable searches being undertaken. Nor can a government sworn to protect the Constitution and laws of the United States ever justify flouting the constitutional amendments and laws that were set up precisely to protect our hard-won human rights.

Thank you. I stand ready to answer any qeustions the Committee may have.

1 A summary of my views on the constitutional law governing national security can be found, inter alia, in HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR (1990). A brief curriculum vitae is attached as an appendix to this testimony. Although I sit on a law school faculty as well as on the boards of numerous organizations, the views expressed here are mine alone.
2 See, e.g., Prepared Statement of Hon. Alberto R. Gonzales, Att'y Gen. of the United States, Feb. 6, 2006, available at http://www.usdoj.gov/ag/speeches/2006/ag_speech_060206.html; U.S. Dept. of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006) [hereinafter DOJ White Paper] (setting forth, after the fact, the Department's analysis of the legal basis for the terrorist surveillance program); Letter from William E. Moschella, Asst. Att'y Gen., Office of Legislative Affairs to Hon. Pat Roberts, Chairman, S. Select Comm. on Intelligence (Dec. 22, 2005).
3 I served as an Attorney-Adviser at the Office of Legal Counsel of the U.S. Department of Justice from 1983-85, and as Assistant Secretary of State for Democracy, Human Rights and Labor from 1998-2001.
4I appeared as private counsel challenging U.S. government actions, inter alia, in Sale v. Haitian Centers Council, Inc., 509 U.S. 155 (1993) (interdiction of Haitian refugees); Cuban-American Bar Ass'n v. Christopher, 43 F.3d 1413 (11th Cir. 1995) (detention of Cuban refugees on Guantanamo).
5 I believe that my opinion is widely shared in the legal community. To give just three examples, I direct the Committee's attention first: to two detailed letters, which I co-signed, recently sent to Members of Congress by fourteen constitutional law scholars and former government officials regarding the illegality of the NSA domestic surveillance program. See Beth Nolan, Curtis Bradley, David Cole, Geoffrey Stone, Harold Hongju Koh, Kathleen M. Sullivan, Laurence H. Tribe, Martin Lederman, Philip B. Heymann, Richard Epstein, Ronald Dworkin, Walter Dellinger, William S. Sessions, William Van Alstyne, On Nsa Spying: A Letter To Congress, available at http://www.nybooks.com/articles/18650; http://balkin.blogspot.com/FISA.DOJ.Reply.pdf; second, to the Resolution of the ABA House of Delegates and Task Force Report of the ABA Task Force on Domestic Surveillance in the Fight Against Terrorism (to which I served as Special Advisor) dated Feb. 13, 2006, available at http://www.abanet.org/op/domsurv/ (resolving inter alia "that the American Bar Association opposes any future electronic surveillance inside the United States by any U.S. government agency for foreign intelligence purposes that does not comply with the provisions of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq. (FISA), and urges the President, if he believes that FISA is inadequate to safeguard national security, to seek appropriate amendments or new legislation rather than acting without explicit statutory authorization."); and third, to the similar conclusion reached by the Congressional Research Service, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information (Jan. 5, 2006), available at http://www.fas.org/sgp/crs/intel/m010506.pdf.
6 U.S. Const., amend. IV.
7 Act. of Oct. 25, 1978, Pub. L. No. 95-511, 92 Stat. 1783.
8 U.S. Const., art. II, sec. 3.
9 U.S. v. Smith, 27, F. Cas. 1192, 1230 (C.C.D.N.Y. 1806) (No. 16,342) (Paterson, J., Circuit Justice).
10 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638 (1952) (Jackson, J., concurring).
11 The Administration claims that the very discussion of these matters before this Committee and elsewhere has compromised the NSA's ability to get its important job done. But if the Administration had only stayed within the four corners of the FISA and sought additional statutory authority as necessary, we would not be here discussing these important issues.
12 Joint Resolution of Aug. 10, 1964, Pub. L. No. 88-408, 78 Stat. 384 (1964). Repealed by Act of Jan. 12, 1971, Pub. L. No. 91-672, § 12, 84 Stat. 2053 (1971).
13 To give just a few examples, the "Rockefeller Commission" investigation into CIA activities within the United States found that in 1972, the CIA examined some 2.3 million pieces of mail, and opened some 8,700 of them. Much of the mail examined and opened was selected based on "watch lists" the agency had developed. The Comm'n on CIA Activities within the United States: Report to the President 111-12 (1975). Available at: http://www.history-matters.com/archive/church/rockcomm/contents.htm (last visited Feb. 26, 2006). Under "Operation CHAOS," the CIA gathered files on more than 7,000 US citizens, containing the names of more than 300,000 persons and organizations. Id. at 23. The "Church Committee" found that Presidents Johnson and Nixon had requested and received information on antiwar activists, political critics, and even members of Congress. The Committee also discovered that the FBI had engaged in virtually unsupervised electronic wiretapping, including bugs that were famously placed in the hotel rooms of the late civil rights leader Dr. Martin Luther King, Jr. Select Comm. to Study Gov't Operations with respect to Intelligence: Final Report, S. Rep. No. 755, 94th Cong., 2d Sess. (1976).
14 50 U.S.C. § 1809 (2000).
15 18 U.S.C. § 2511(2)(f) (West 2002) (emphasis added).

1650 U.S.C. § 1801. (West. 2004). Although the emergency wiretap period was originally only 24 hours, after September 11, 2001, the Bush Administration specifically requested and received the increase to 72 hours. See Pub.L. No. 107-108, 115 Stat. 1394 (2001).
17 50 U.S.C. § 1811. The House version of the bill would have authorized the President to conduct warrantless electronic surveillance for one year after a declaration of war, but the Conference Committee expressly rejected that suggestion, reasoning that the 15-day "period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. Conf. Rep. No. 95-1720, at 34 (1978). "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." Id.
18 Annual reports of the FISA Court available at http://www.fas.org/irp/agency/doj/fisa/#rept (last visited Feb. 26, 2006).
19 Id.
20 "[A]ny time you hear the United States government
talking about wiretap, it requires -- a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so." President George W. Bush, Information Sharing, Patriot Act Vital to Homeland Security (April 20, 2004), available at http://www.whitehouse.gov/news/releases/2004/04/20040420-2.html; "[T]he government can't move on wiretaps or roving wiretaps without getting a court order." President George W. Bush, President's Remarks at Ask President Bush Event (July 14, 2004), available at http://www.whitehouse.gov/news/releases/2004/07/20040714-11.html; "Law enforcement officers need a federal judge's permission to wiretap a foreign terrorist's phone, a federal judge's permission to track his calls, or a federal judge's permission to search his property. Officers must meet strict standards to use any of these tools. And these standards are fully consistent with the Constitution of the U.S." President George W. Bush, President Discusses Patriot Act (June 9, 2005), available at http://www.whitehouse.gov/news/releases/2005/06/20050609-2.html.
21 A Hearing of the Senate Judiciary Committee: Nomination of Alberto Gonzales to be Attorney General, 109th Cong. (Jan. 6, 2005) (statement of Alberto Gonzales). He added that he would hope to alert Congress if the president ever chose to authorize warrantless surveillance. Id.
22 James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers without Courts, N.Y. Times, Dec. 16, 2005, at A1.
23Just six weeks after September 11, Congress passed the USA PATRIOT Act to expand the government's powers to conduct surveillance of suspected terrorists. See Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. Yet the Administration never asked for, nor did the Patriot Act include, any change to FISA's requirement that courts give warrants before Americans in the United States can be wiretapped.
24 Daniel Klaidman, et al., Palace Revolt, NEWSWEEK, February 6, 2006, available at http://www.msnbc.msn.com/id/11079547/site/newsweek/.
25 James Risen, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 48-53 (2006).
26 See, generally, id; 50 U.S.C. § 1805(a) (provision of FISA requiring that a subject be "the agent of a foreign power").
27 As Attorney General Gonzales said in his testimony before this Committee, "the program is triggered only when a career professional at the NSA has reasonable grounds to believe that one of the parties to a communication is a member or agent of al Qaeda or an affiliated terrorist organization." Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the Senate Judiciary Comm., 109th Cong. (Feb. 6, 2006) (statement of Alberto Gonzales) (hereinafter NSA Hearing).
29 See NSA Hearing, supra note 26 (statement of Alberto Gonzales); 50 U.S.C. §§ 1801(f)(1)-(2), 1801(n). See also Letter from William E. Moschella to Senator Pat Roberts et. al. (Dec. 22, 2005), supra note 1 at 4.
30 See Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), at http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html.
31 Id.
32 See Wartime Executive Power and the NSA's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary, 109th Cong. (2006) (Joint Statement of John M. Harmon, Asst. Att'y Gen., Office of Legal Counsel, Dept. of Justice 1977-1981 and Larry L. Simms, Dep. Asst. Att'y. Gen., Office of Legal Counsel, Dept. of Justice 1979-1985) ("Indeed, it is quite unclear from the Administration's various factual assertions whether any written legal advice was received by the President or his then Counsel, now the Attorney General, before the program was implemented. ...Congress has a right to understand what advice the President acted upon in 2001 when the program was implemented ....).

33 343 U.S. 579 (1952).
34 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring)(emphasis added). In Dames & Moore v. Regan, 453 U.S. 654 (1981), the entire Supreme Court embraced Justice Jackson's view as "bringing together as much combination of analysis and common sense as there is in this area." Id. at 661 (Rehnquist, C.J.).
35 DOJ White Paper at 6-10, 28-36.
36 See United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 321-25 (1972).
37 343 U.S. 579, 643-44 (Jackson, J., concurring).
38 U.S. Const., art. I, § 8, cl. 14; U.S. Const., art. I, §18.
3918 U.S.C. §§ 2340-2340A (torture); Pub. L. No. 109-148, Div. A, tit. X, § 1003, 119 Stat. 2739-2740 (2005) (cruel, inhuman, and degrading treatment).
40 Indeed, the relevant precedents are all to the contrary. See, e.g., Hamdi v. Rumsfeld, 542 U.S. 507, 535-36 (2004) (rejecting the President's claim that courts may not inquire into the factual basis for detention of a U.S. citizen "enemy combatant," reasoning that "[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."); Rasul v. Bush, 542 U.S. 466 (2004) (rejecting the President's claim that it would be an unconstitutional interference with the President's Commander-in-Chief power to interpret the habeas corpus statute to encompass actions filed on behalf of Guantanamo detainees); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 586 (1952) (invalidating the President's seizure of the steel mills where Congress had previously "rejected an amendment which would have authorized such governmental seizures in cases of emergency."); Ex parte Milligan, 71 U.S. (4 Wall.) 2 (1866) (holding that the Executive had violated the Habeas Corpus Act by failing to discharge from military custody a petitioner charged, inter alia, with violation of the laws of war); Little v. Barreme, 6 U.S. (2 Cranch) 170 (1804) (invalidating a presidential seizure of a ship during a conflict with France as implicitly disapproved by Congress); United States v. Smith, 27 F. Cas. 1192, 1218 (C.C.D.N.Y. 1806) (No. 16,342) (Paterson, J., Circuit Justice) ("[t]he president of the United States cannot control the statute, nor dispense with its execution, and still less can he authorize a person to do what law forbids.").
41 While the Foreign Intelligence Surveillance Court of Review suggested in dictum in In re Sealed Case No. 02-001, 310 F.3d 717, 742 (FIS Ct. Rev. 2002) (per curiam) that Congress cannot "encroach on the President's constitutional power" to conduct foreign intelligence surveillance, the court in that case upheld FISA's constitutionality, affirming that Congress may constitutionally regulate significant amounts of foreign intelligence without entrenching on exclusive presidential prerogatives.
42 343 U.S. 579, 637 (1952) (Jackson, J., concurring)(emphasis added): id. at 644 (Jackson, J., concurring) ("That military powers of the Commander in Chief were not to supersede representative government of internal affairs seems obvious from the Constitution and from elementary American history. ... [T]he Constitution's policy [is] that Congress, not the Executive, should control utilization of the war power as an instrument of domestic policy.").
44 Pub. L. No. 107-40, § 2 (a), 115 Stat. 224, 224 (Sept. 18, 2001).
45 J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc., 534 U.S. 124, 141-42 (2001) ("'[T]he only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable.'") (citing Morton v. Mancari, 417 U.S. 535, 550 (1974)). The AUMF and § 2511(2)(f) are not irreconcilable, and there is no evidence, let alone overwhelming evidence, that the AUMF intended to repeal this section of FISA.
46 Press Release, The White House, Office of the Press Secretary, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at www.whitehouse.gov/news/releases/2005/12/20051219-1.html.
47 Indeed, when the Attorney General made this claim to this Committee, Senator Lindsey Graham correctly called this argument "very dangerous in terms of its application for the future....I'll be the first to say that when I voted for [the AUMF], I never envisioned that I was giving to this president or any other president the ability to go around FISA carte blanche." http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601001.html In Gonzales v. Oregon, 126 S. Ct. 904 (Jan. 17, 2006), Justice Kennedy, writing for the Court, recently rejected the parallel "idea that Congress gave the Attorney General such broad and unusual authority through an implicit delegation in" a federal statutory registration provision. Id. at 921. "'Congress, we have held, 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.'" Id. (quoting Whitman v. American Trucking Assns., Inc., 531 U.S. 457, 468 (2001)). Neither, one might add here, does Congress hide repeals of major national security framework statutes in the cryptic words "necessary and appropriate force."
48 See 50 U.S.C. § 1811 (2000) (15 day window); 18 U.S.C. § 2511(2)(f) (2000) (exclusivity). Such specific and "carefully drawn" statutory language prevails over general statutes, such as the AUMF, where there is a conflict. Morales v. Trans World Airlines, Inc., 504 U.S. 374, 385 (1992) (quoting International Paper Co. v. Ouelette, 479 U.S. 481, 494 (1987)).

49 Youngstown, 343 U.S. at 609 (Frankfurter, J., concurring).
50 542 U.S. 507 (2004).
51 Hamdi, 542 U.S. at 516-19 (emphasis added).
52 Id. at 520.
53 As Tom Daschle, who as Senate Majority Leader negotiated with the Administration regarding the text of the AUMF, has written:

I can state categorically that the subject of warrantless wiretaps of American citizens never came up. I did not and never would have supported giving authority to the president for such wiretaps. I am also confident that the 98 senators who voted in favor of authorization of force against al Qaeda did not believe that they were also voting for warrantless domestic surveillance....Literally minutes before the Senate cast its vote, the administration sought to add the words "in the United States and" after "appropriate force" in the agreed-upon text. This last-minute change would have given the president broad authority to exercise expansive powers not just overseas...but right here in the United States, potentially against American citizens. I could see no justification for Congress to accede to this extraordinary request for additional authority. I refused....The Bush administration now argues those powers were inherently contained in the resolution adopted by Congress -- but at the time, the administration clearly felt they weren't or it wouldn't have tried to insert the additional language.

Tom Daschle, Power We Didn't Grant, WASH. POST, Dec. 23, 2005, A21. See also 147 CONG. REC. H5675 (daily ed. Sept. 14, 2001) (statement of Rep. Jackson) ("I am not voting 'Yes' on September 14, 2001, for an open-ended Tonkin Gulf-type Resolution. . . . I'm not willing to give President Bush carte blanche authority to fight terrorism.")
54 Transcript available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (last viewed Feb. 26, 2006).
55 Some administration officias have denied a "driftnet" or "data-mining" operation. See, e.g., Michael Hayden, Address to the National Press Club: What American Intelligence and Especially the NSA Have Been Doing to Defend the Nation, Jan. 23, 2006, available at http://www.dni.gov/release_letter_012306.html).
However, the number and consistency of media reports in the media over the past three months based on interviews with informed government officials provide cause for concern that a broader operation is indeed underway, and places a burden upon the Administration to explain how the surveillance operation is in fact kept limited.
56 James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y.Times, Dec. 16, 2005, A1; Spy Agency Mined Vast Data Trove, Officials Report, N.Y. Times, December 24, 2005, A1. See also, James Risen, State of War: the Secret History of the CIA and the Bush Administration 44 (2006): "The NSA is now tapping into the heart of the nation's telephone network through direct access to key telecommunications switches that carry many of America's daily phone calls and email messages. O]ne indication of [the program's] large scale is the fact that administration officials say that one reason they decided not to seek court-approved search warrants for the NSA operation was that the volume of telephone calls and e-mails being monitored was so big that it would be impossible to get speedy court approval for all of them." Id., at 48.
57 Barton Gellman, Dafna Linzer and Carol D. Leonnig, Surveillance Net Yields Few Suspects, WASH. POST, Feb. 5, 2006, at A1.
58 Dec. 19 Press Briefing, Transcript available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (last viewed Feb. 26, 2006).
59 Given that the FISA scheme was designed precisely to protect those rights, these constitutional concerns further weigh against an overbroad interpretation of the AUMF that would silently repeal FISA.
60 See 9/11 COMMISSION REPORT at 79 ("Agents in the field began to believe--incorrectly--that no FISA information could be shared with agents working on criminal investigations. This perception evolved into the still more exaggerated belief that the FBI could not share any intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators. Separate reviews in 1999, 2000, and 2001 concluded independently that information sharing was not occurring.").
61 Letter from Senator Jay Rockefeller to Vice President Cheney, July 17, 2003, available at http://www.globalsecurity.org/intell/library/news/2005/intell-051219-rockefeller01.pdf (last viewed: Feb. 27, 2006).
62 For intelligence activities generally, including any significant anticipated intelligence activity other than covert action, the National Security Act of 1947 requires that "the congressional intelligence committees" are to be kept "fully and currently informed" of such activities. 50 U.S.C. § 413 (a)(1) (2000). See also ALFRED CUMMING, CONGRESSIONAL RESEARCH SERVICE, STATUTORY PROCEDURES UNDER WHICH CONGRESS IS TO BE INFORMED OF U.S. INTELLIGENCE ACTIVITIES, INCLUDING COVERT ACTIONS 3-6 (2006)). By law, covert actions require a formal presidential "finding," one that must be then shared with the Gang of Eight. There has been

no assertion that the President issued such a finding in the case of the NSA domestic surveillance program; if he indeed has not, then the Administration had no basis in law for limiting its briefings to the Gang of Eight.
63 U.S. CONST. art. I § 8 cls. 12, 14; § 9 cl. 7.
64 50 U.S.C. 413(a)-(b) (2000). Finally, even when such limited notice is given, the President is still required to report "in a timely fashion." Id.
65 This is especially true when one of the few briefed, the Ranking Member on the House Permanent Select Committee on Intelligence, has publicly stated that: "I am one of the few in Congress who has been briefed on the program, and I am not clear why FISA as presently drafted cannot cover the entire program." See Letter from Rep. Jane Harman to President George W. Bush, Feb. 1, 2006, available at http://www.house.gov/harman/press/releases/2006/0201PR_fisawarrants.html
66 SENATOR FEINGOLD: Do you know of any other president who has authorized warrantless wiretaps outside of FISA since 1978 when FISA was passed? AG GONZALES: None come to mind, Senator, but I'd be happy to look to see whether or not that's the case. Transcript, NSA Hearing, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601359.html
67 50 U.S.C. § 1805(a)(3) (2000)
68 Proposed NSSA, § 704(3) (emphasis added).
69 I am a board member of the National Democratic Institute (NDI), an American democracy nongovernmental organization that frequently makes contact with Middle Eastern foreign governments as part of pro-democracy work abroad. Read literally, this bill could authorize a surveillance program whereby NDI workers in contact with foreign government workers in connection with election monitoring could have all their e-mails and telephone conversations with anyone tapped, for a minimum of 90 days.
70Although under the bill "continuous" surveillance could only last 90 days, there is no apparent bar to the NSA simply waiting a few days then starting the surveillance anew.
71 Also curious is the bill's Section 704, which directs the FISA court to consider the benefits of a particular program "as reflected by the foreign intelligence information obtained." This is a judgment, calling in effect for an advisory opinion, which is far more appropriate for a legislative committee than for an Article III court tasked with deciding cases or controversies.
72 It is true that a line of Fourth Amendment cases permits warrantless search programs to further certain "special needs," such as drunk driving checkpoints and urine testing in schools. But when such practices have been sustained, courts have concluded that alternative search processes are reasonable, because the searches are generally brief, minimally intrusive, standardized, and there is a demonstrated government need to dispense with individualized warrants and probable cause. See, e.g., Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (upholding drunk driving checkpoints); Vernonia Sch. Dist. v. Acton, 515 U.S. 646 (1995) (upholding school drug testing). The NSA spying program, by contrast-- and the kind of "surveillance pro