



National Security Law Report

Special Issue: The NSA Surveillance Debate

Revelations concerning a program of warrantless surveillance conducted by the National Security Agency have prompted sharp debate around the country in recent weeks. The new editor of the National Security Law Report, Professor Robert Chesney of Wake Forest University School of Law, has assembled a series of seven essays debating the legal issues raised by these revelations. Contributors William Banks, Suzanne Spaulding, and David Cole present criticisms of the program, while contributors Brian Boyle, Robert Turner, and Andrew McCarthy defend its legality. Finally, Richard Friedman provides concluding observations.

“If Men Were Angels”

NSA Eavesdropping and the Fourth Amendment

William Banks

Madison’s famous defense of separated government powers in *The Federalist* recognized that, being far from angels, those who governed had to be controlled by laws. President Bush’s order permitting the National Security Agency (NSA) to eavesdrop on Americans without any judicial approval or warrant shows Madison’s prescience. In this instance, the legal controls were present – the Foreign Intelligence Surveillance Act (FISA) process that allows for secret judicial authorization to conduct the sort of electronic eavesdropping being conducted by NSA – but they were circumvented. The civil liberties dimensions of the NSA program have taken a legal back seat to the constitutional and statutory authority issues in these debates. Still, in the unlikely event that legal authority for the NSA program can be found, this domestic spying violates the Fourth Amendment.

Administration lawyers concede that, in general, individuals have a reasonable expectation of privacy in their telephone calls, and that probable cause and a warrant are necessary under the Fourth Amendment to

Seller’s Remorse?

The Authorization for Use of Military Force in the NSA Surveillance Debate

Brian D. Boyle

It doesn’t take an overactive imagination to surmise that terrorist partisans, hoping to stage another attack on United States soil, are regularly making international calls or sending international e-mail to persons in this country. The purposes of these calls may vary from simply acquiring intelligence from innocent, unsuspecting individuals about the accessibility of “soft” targets, to attempting to recruit United States persons to terrorist operations, or even to coordinating with al Qaeda affiliates already recruited to the terrorists’ ends. President Bush’s assertion that an effective defense against the terrorists must include the monitoring of their international communications to and from the United States seems quite reasonable against this assumption. Congress, in the Authorization for Use of Military Force (“AUMF”) enacted shortly after 9-11, both acknowledged the President’s inherent authority to “deter and prevent” further attacks against the United States, and authorized the President “to use all necessary and appropriate force against those ... he determines planned, authorized, committed, or aided”

If Men Were Angels...

Continued from page 1

authorize electronic surveillance of those communications. The extent to which national security and foreign intelligence collection might be exempt from the general rule and thus subject to the lesser Fourth Amendment requirement of reasonableness has been considered carefully if not exhaustively by Congress and the judiciary. Thirty-four years ago the Supreme Court first confronted the tensions between unmonitored executive surveillance and individual freedoms in the national security setting. *United States v. United States District Court* arose from a criminal proceeding in which the United States charged three defendants with conspiracy to destroy government property – the dynamite bombing of a CIA office in Ann Arbor, Michigan. During pretrial proceedings, the defendants moved to compel disclosure of electronic surveillance. The Government admitted that a warrantless wiretap had intercepted conversations involving the defendants. In the Supreme Court, the government defended its actions on the basis of the Constitution and a national security disclaimer in the 1968 Crime Control Act. Justice Powell’s opinion for the Court first rejected the statutory argument and found that the Crime Control Act disclaimer of any intention to legislate regarding national security surveillance simply left presidential powers in the area untouched.

Turning to the constitutional claim, the Court found authority for national security surveillance implicit in the President’s Article II Oath Clause, which includes the power “to protect our Government against those who would subvert or overthrow it by unlawful means.” However, the “broader spirit” of the Fourth Amendment, and “the convergence of First and Fourth Amendment values” in national security wiretapping cases made the Court especially wary of possible abuses of the national security power. Justice Powell then proceeded to balance “the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression.”

Although the government argued for an exception to the warrant requirement, citing the unique characteristics of ongoing national security surveillance, Justice

Powell answered that the potential for abuse of the surveillance power in this setting, along with the capacity of the judiciary to manage sensitive information in *ex parte* proceedings, rendered any inconvenience to the government “justified in a free society to protect constitutional values.”

Justice Powell was careful to emphasize that the case involved only the domestic aspects of national security, and that the Court was not expressing an opinion on the discretion to conduct surveillance when foreign powers or their agents are targeted. Finally, the Court left open the possibility that different warrant standards and procedures than those required in normal criminal investigations might be applicable in a national security investigation, implicitly inviting Congress to promulgate a set of standards for such surveillance:

Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of the citizen rights deserving protection.

Justice Powell’s opinion provided an important impetus

THE ABA NATIONAL SECURITY LAW REPORT

<<http://www.abanet.org/natsecurity/>>

EDITORIAL BOARD

Suzanne E. Spaulding
Stewart Baker
Richard E. Friedman
Elizabeth Rindskopf Parker
Pamela Parizek
Holly Stewart McMahon
Robert M. Chesney, *Editor*

The *National Security Law Report* (N.S.L.R.) contains articles concerning the law relating to the security of our Nation and associated topics. The N.S.L.R. is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise.

To receive the N.S.L.R., contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; FAX (202) 662-1032; or hmcMahon@staff.abanet.org.

for the development of what became FISA. Like the Supreme Court, Congress recognized that warrantless surveillance by the executive branch untethered by law could undermine important constitutional values at the confluence of the First and Fourth Amendments. FISA thus became a sort of constitutional compromise between adherence to the traditional law enforcement warrant and probable cause requirements and those who sought authority for warrantless surveillance. Instead of the traditional law enforcement warrant and probable cause, FISA requires the government to show that it seeks foreign intelligence and that there is probable cause to believe that the target of the surveillance is an agent of a foreign power. All of the federal courts that reviewed the constitutionality of FISA upheld it against the Fourth Amendment challenge, and no court has upheld warrantless electronic surveillance since the enactment of FISA.

Congress made clear in FISA that its requirements provide the “exclusive” means for obtaining an order to engage in wiretapping in the United States in pursuit of foreign intelligence. In effect, the Administration was boxed in by Congress and FISA on the Fourth Amendment. If Congress had not responded to Justice Powell with a compromise scheme, refusing claims for executive branch authority to go it alone in foreign intelligence collection would be difficult to defend in today’s climate. Now, the proponents of the NSA program are left with the unconvincing arguments that FISA is too cumbersome, or that the statute unconstitutionally limits the Commander in Chief.

The only justification offered by the Administration that the NSA program complies with the Fourth Amendment is a weak one, borrowed from the opinion of the FISA Court of Review in its *In re Sealed Case* decision in 2002. The argument is that the NSA program may be fitted within a line of Fourth Amendment cases excepting from the warrant and probable cause requirements situations where the government has “special needs” above and beyond ordinary law enforcement. The “special needs” category has sustained drunk-driving checkpoints and drug testing in schools, programs that are relatively non-intrusive and standardized. “Special needs” has never been extended to the highly intrusive and wholly discretionary warrantless wiretapping. As the FISA Court of Review recognized in *upholding* FISA, the FISA system

for obtaining judicial approval based on individualized suspicion is workable and lawful.

If the NSA program was designed to listen in on known al Qaeda members or affiliates who are U.S. persons, as first claimed by the Administration, it is not difficult to imagine FISA judges issuing orders for such surveillance, following a FISA judge’s finding that there is probable cause to believe that the targets are agents of a foreign power. As congressional hearings and continued reporting expand our knowledge of the NSA program, it appears that the surveillance was not necessarily limited to known al Qaeda members or affiliates. If instead, or in addition, the NSA program involves data mining – identifying persons of interest from among the general population, rather than listening in on persons of interest already identified – the government’s unwillingness to follow the FISA process for the data mining makes more sense. From the mined data, however, NSA still presumably identifies individuals who could be targeted through the FISA means.

The President assures us that the NSA program protects civil liberties. On this one, I’ll cast my lot with Madison. Following Justice Powell, the inconvenience of a judicial role in monitoring this program is “justified in a free society to protect constitutional values.”

William Banks is the Laura J. and L. Douglas Meredith Professor for Teaching Excellence at Syracuse University College of Law, the Director of Syracuse’s Institute for National Security and Counter Terrorism, and co-author of the casebook National Security Law (4th ed.).

Seller’s Remorse...

Continued from page 1

the 9-11 attacks. The surveillance program the President has described – involving international communications to and from the United States where there is a “reasonable basis to conclude that one party to the communication is” affiliated with al Qaeda – would seem to fit comfortably within this congressional authorization.

In prior conflicts, Presidents have not hesitated to apply their Constitutional powers as the Nation’s Command-

Continued on page 4

Seller's Remorse...

Continued from page 3

er in Chief to commence monitoring – indeed, outright censorship – of just such communication links between persons in the U.S. and persons in enemy territory. President Wilson issued Executive Order 2604 in April 1917, commanding telegraph and telephone companies to cease transmitting international communications to and from the U.S. except pursuant to rules and regulations promulgated by the War Department. Immediately after the attack on Pearl Harbor, President Roosevelt authorized interception of all “communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country.” Such monitoring was not targeted at particular U.S. persons, or even particular persons in enemy territory. Instead, Presidents have historically applied their Commander in Chief powers systematically to cull international communications traffic between the U.S. and persons under the nominal control of our enemies to guard against the one in a thousand possibility that our Nation’s secrets were being transmitted outbound, or that enemy plans for stateside operations were being staged.

While Congress plainly authorized the use of military force in these prior conflicts (just as with the AUMF), it did not explicitly authorize the President to engage in surveillance operations involving international communications to and from the U.S. Either such authorization was implied, or the President was left to his Article II powers to carry out such intelligence operations. Congress certainly did not purport to prohibit such intelligence collection, any more than it sought to constrain how the Commander in Chief maneuvered the country’s Naval Forces. Indeed, any such attempt by Congress to require the President to prohibit the acquisition and use of foreign intelligence in conducting military operations, or to prohibit such deployment of the Armies and Naval Forces that Congress has “raised” or “provide[d] for” in the manner that the President determines will best provide for the defense of the country, would – as Andrew McCarthy’s essay underscores – raise grave questions concerning whether Congress was intruding on the President’s Commander in Chief powers under Article II of the Constitution.

Nevertheless, some say that the Foreign Intelligence

Surveillance Act was intended to do just that – to place certain means of collecting foreign intelligence beyond the President’s reach, even in wartime. They argue that, under FISA’s plain language, “electronic surveillance” involving a “United States person,” in which the contents of communications are acquired from within the United States, can only be commenced if there is “probable cause” to believe that such person is an agent of a “foreign power” (defined to include a terrorist organization), and a federal judge so finds – either prior to the commencement of the surveillance or within 72 hours thereafter if emergency circumstances require commencement while a warrant request is under preparation. They also point to conforming amendments added to Title 18 of the U.S. Code at the time of FISA’s enactment stating that FISA and Title III of the Omnibus Crime Control Act constitute the “exclusive means” by which “electronic surveillance” (as defined in FISA) “may be conducted.” 18 U.S.C. § 2511(2)(f). This latter provision would be rendered nugatory by the President’s interpretation of the AUMF, they say, violating an important canon of statutory construction.

But canons of statutory construction are simply interpretive aids; they allow courts to select from among competing interpretations of a statute where an ambiguity cannot otherwise be resolved. Here, however, a larger principle is at stake – that of respect for the President’s powers as Commander in Chief in time of war, and for the unbroken Executive tradition of prophylactic monitoring of communications into and out of our country involving enemy partisans or territory. Under the principle of constitutional avoidance, a construction of FISA and the AUMF together that avoids interference with Presidential prerogatives to screen enemy contacts with persons in the United States in time of war – interference that would raise serious questions under Article II – is to be strongly favored. A conclusion that the AUMF authorizes the President to engage in such traditional screening of communications between enemy personnel and persons in the United States as he thinks necessary to “deter and prevent” further terrorist attacks on the Nation’s soil avoids such Article II concerns. And while the Congress that enacted FISA in 1978 declared that FISA and the provisions of Title 18 constitute the “exclusive” vehicles for authorizing surveillance, that pronouncement could not have bound the later Congress that enacted

the AUMF. In any event, FISA itself alludes to the possibility of a separate statutory grant of authority by excepting from its criminal prohibition surveillance that is “authorized by statute.” 50 U.S.C. § 1809(a)(1).

Some in Congress who voted for the AUMF dissent from the notion that Congress intended to affirm the President’s wartime surveillance powers. Many of these also question whether the AUMF was intended to permit the President to detain American citizens captured in the war on terror as enemy combatants (a form of seller’s remorse, perhaps). But in *Hamdi*, the Supreme Court affirmed the President’s power to detain citizen combatants by construing the expansive language of the AUMF in the light of the President’s historical exercise of his powers as Commander in Chief, finding the general grant of authority sufficiently broad to overcome a separate act of Congress prohibiting detention of U.S. citizens “except pursuant to an act of Congress.” 18 U.S.C. § 4001(a). There is no basis to treat the former question any differently.

Now that the general aspects of the President’s surveillance program are public, Congress is certainly at liberty to trim the powers affirmed in the AUMF, perhaps forcing constitutional questions to the fore. In our constitutional system, of course, Congress’s view on the proper scope of NSA’s surveillance activities must ultimately prevail – if nothing else, when Congress refuses to continue appropriations for the activities. Yet the public debate over the lawfulness of the President’s program has obscured the important question whether the Nation’s security demands precisely the kind of screening of enemy contacts with U.S. persons that the NSA is conducting. Judged by the wartime actions of Presidents past, there are compelling reasons to believe it does. FISA’s procedures – assuming they occupy the field – simply do not allow such prophylaxis; as emphasized, FISA demands “probable cause” that the U.S. party to any monitored communications is an agent of a “foreign power.” If and when Congress reconsiders the scope of the AUMF, let’s hope that our Nation’s historical experience in waging war is not forgotten.

Brian Boyle, currently a partner at O’Melveny & Myers LLP, served from 2003 to 2005 as a Principal Deputy Associate Attorney General in the De-

partment of Justice, and previously served as an Assistant General Counsel in the Office of the Secretary of the Army.

The Statutory Argument in the NSA Surveillance Debate

Suzanne E. Spaulding

The Administration has conceded that the electronic surveillance program authorized by the President after the attacks of 9/11 falls within the definitions of the Foreign Intelligence Surveillance Act (FISA) but is not being conducted pursuant to the procedural requirements of that statute. Nevertheless, it argues that NSA’s warrantless surveillance inside the United States does not violate FISA because the Authorization for the Use of Force (AUMF) enacted after 9/11 provides the necessary statutory authorization. This argument is not supported by traditional methods of statutory construction, Congressional intent, or Supreme Court precedent.

Under FISA, it is a crime to conduct electronic surveillance inside the United States “unless otherwise authorized by statute.” Thus, surveillance conducted pursuant to FISA or the criminal wiretap statute is clearly authorized. The Administration asserts that the AUMF also qualifies as a statute that authorizes electronic surveillance, despite the absence of any reference in the resolution to such activity.

The resolution enacted after 9/11 authorized the President to “use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks.” The Administration argues that this AUMF implicitly authorized the warrantless surveillance of Americans who may be talking to terrorists because electronic surveillance of the enemy is a fundamental and traditional incident of the use of military force. Thus, the argument goes, when Congress authorized the use of force, they also intended to authorize everything that goes with it, including wire-

Continued on page 6

The Statutory Argument...

Continued from page 5

tapping Americans inside the US who might be in contact with al Qaeda or affiliates.

Yet, when Congress enacted FISA, they specifically contemplated how it would work in war time and included a provision allowing warrantless searches for up to 15 days after the declaration of war. If even a formal declaration of war had this limited effect, it is hard to see how a resolution authorizing the use of force can be viewed as intended to authorize warrantless surveillance for an unlimited period of time.

Moreover, the Members of Congress themselves have indicated that they did not intend to grant the authority asserted by the Administration. Former Senator Tom Daschle, who was Democratic Leader of the Senate when the AUMF was passed, has written that the Administration sought to have the resolution broadened to apply inside the US and Congress refused. Other senators have also expressed the view that they did not intend to authorize warrantless surveillance of Americans in the AUMF.

Traditional rules of statutory construction also support a more limited reading of the AUMF. Courts generally will not view a specific statutory prohibition such as that found in FISA as having been overruled by a more general statute such as the AUMF, particularly without a clear indication that Congress intended that result.

The Administration cites the Supreme Court's decision in the *Hamdi* case to support its broad reading of the AUMF. That case involved the detention of a US citizen on the battlefield in Afghanistan and his detention as an enemy combatant. Hamdi argued that his detention violated the Non-Detention Act, 18 USC 4001(a), which provides that no U.S. citizen may be detained except pursuant to an act of Congress. Justice Sandra Day O'Connor wrote the plurality opinion, which determined that detention of the enemy is such a traditional aspect of war fighting that it is implicitly authorized by the AUMF. The *Hamdi* decision is distinguishable on several grounds, including the nature of the statutes, the conflict, and the government's activity.

The statute at issue in *Hamdi* is one sentence long and clearly contemplates that there will be other statutes authorizing detentions. In contrast, FISA sets out a long, detailed statutory framework covering a wide range of circumstances, including war. It explicitly states that it is "the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." Finding an implicit authorization to operate outside this legal framework presents a tougher burden than was the case with *Hamdi* and the Non-Detention Act.

Moreover, the *Hamdi* decision emphasizes the difference between a traditional armed conflict like the war in Afghanistan, which was the context in which Hamdi was detained, and the more amorphous, long-term "global war on terrorism" that provides the context for the warrantless surveillance of the NSA program. As Justice O'Connor explained in *Hamdi*, "we understand Congress' grant of authority for the use of 'necessary and appropriate force' to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel."

The Court cited the Geneva Conventions and other international laws to support its conclusion that the use of armed force clearly contemplates the capture of enemy combatants. It is difficult to conceive of Congress authorizing the President to engage in armed conflict overseas but not intending to give him the authority to capture enemy soldiers. However, the same cannot be said of electronic surveillance of American citizens inside the United States, particularly in light of a contrary statute.

In fact, the Justices, aside from Justice Thomas, expressed skepticism about the Administration's claims based on intelligence needs. Justice O'Connor agreed that the law of war supports detention of enemy combatants to prevent their return to the battlefield, but stated that "indefinite detention for the purpose of interrogation is not authorized." Similarly, while collecting intelligence against the enemy is an essential element of war fighting, it does not automatically follow

that the same analysis applies to a program for intercepting emails and phone calls of Americans inside the United States whenever an NSA shift-supervisor determines that one end of the communication may involve a suspected terrorist.

Once again, the *Hamdi* decision sheds light: “We have long since made clear that a state of war is not a blank check for the president when it comes to the rights of the Nation’s citizens. . . . Whatever power the United States Constitution envisions for the Executive in its exchanges with . . . enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.” That role was not discharged entirely by the mere passage of the AUMF.

Suzanne Spaulding currently is a Principal with the Bingham Consulting Group. She previously served as the Executive Director of both the National Commission on Terrorism and the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, the Minority Staff Director for the House Permanent Select Committee on Intelligence, and as the Deputy Staff Director and General Counsel of the Senate Select Committee on Intelligence. She chaired the Standing Committee from 2001 - 2004.

National Security Law and the NSA-FISA Controversy

Robert F. Turner

It is no credit to our educational system that so many of the President’s critics in the NSA-FISA controversy premise their case not on the undesirability of our government monitoring communications between known or suspected foreign enemies abroad and people in this country (something *every* wartime leader has done since General George Washington authorized surreptitious intercepts of British mail to America, and which few seem to object to on the merits), but rather on the assertion that the Framers of our Constitution demanded that every presidential power be “checked” by Congress or the courts to guard against abuse and the conviction that the President is not “above the law.” To the contrary, it is beyond cavil that the Founding Fathers intended that the new American president would have considerable *unchecked* discretion in such national security areas as military operations, intelligence, and diplomacy – where “secrecy,” “unity of plan,” and “speed and dispatch” were essential, and for which Congress lacked the institutional competency to play a useful role.

Put simply, the framers of our Constitution understood that Congress could not keep secrets. As John Jay explained in *Federalist* No. 64, there were foreign “sources” of “the most useful intelligence” who might

Continued on page 8

Standing Committee on Law and National Security

Chair: Stewart Baker

Members: Eugene Bowman, David Cole, Willie Curtis, Eugene Fidell, Albert Harvey, Philip B. Heymann, Tia Johnson, Wyndee Parker, Michael Posner, Nicholas Rostow, Michael Wermuth

Advisory Committee Chair: Richard E. Friedman

ABA Board of Governors Liaison: Charles A. Powell III

ABA Law Student Division Liaison: John Michael Isom

Staff Director: Holly Stewart McMahan

740 15th St., NW

Washington, D.C. 20005-1009

(202) 662-1035 -- FAX: (202) 662-1032

E-mail: hcmcmahon@staff.abanet.org

Web page: <<http://www.abanet.org/natsecurity>>

National Security Law...

Continued from page 7

assist the new nation if they could be “relieved from apprehensions of discovery,” and many such people simply would not trust the Senate or House to keep secrets. Jay explained that was why the new Constitution had left the president “able to manage *the business of intelligence* in such manner as prudence may suggest.” (Emphasis added.) That the First Congress shared this understanding is apparent from a reading of the first appropriations act for foreign intercourse, which provided that the president should account only “for the *amount* of such expenditures as he may think it advisable not to specify”

When the Founding Fathers wrote in Article 2, section 1, of the Constitution that the “executive power” of the new nation “shall be vested in a President of the United States,” they understood that they were giving their new leader the general management of the nation’s foreign relations. This was a central component of “executive power” found in the writings of men like Locke, Montesquieu, Blackstone. We know this was their understanding because they discussed it often. Thus, in a memorandum to President Washington dated April 24, 1790, Thomas Jefferson reasoned:

The Constitution has declared that “the Executive powers shall be vested in the President,” submitting only special articles of it to a negative by the Senate

The transaction of business with foreign nations is Executive altogether. It belongs then to the head of that department, *except* as to such portions of it as are specially submitted to the Senate. *Exceptions* are to be construed strictly. . . . [Emphasis in original.]

The view was also embraced by Washington, Madison, Jay, Hamilton, John Marshall, and many other key players in our nation’s early history; and this clause was relied upon for nearly two centuries by both branches in excluding Congress from the “business of intelligence.”

On the issue of unchecked presidential discretion, Chief Justice Marshall explained in *Marbury v. Madison* (1803):

By the constitution . . . , the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience. . . . [A]nd whatever opinion may be entertained of the manner in which executive discretion may be used, still there exists, and can exist, no power to control that discretion. The subjects are political. They respect the nation, not individual rights, and being entrusted to the executive, the decision of the executive is conclusive.

In the most famous of all foreign affairs cases, *United States v. Curtiss-Wright Export Corp.* (1936), the Supreme Court referred to “the very delicate, plenary and *exclusive* power of the President as the sole organ of the federal government in the field of international relations,” and explained:

Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of the power is significantly limited. In this vast external realm, . . . the President alone has the power to speak or listen as a representative of the nation. . . . Into the field of negotiation *the Senate cannot intrude, and Congress itself is powerless to invade it.* [Emphasis added.]

Every court of appeals that has considered the issue has held that the president has independent constitutional authority to authorize warrantless foreign intelligence surveillance. In noting this fact in 2002, the appeals court established by FISA declared: “We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President’s constitutional power.” This was also the position taken by Attorney General Griffin Bell on behalf of the Carter Administration when FISA was being enacted in 1978, and when the Clinton Administration asked Congress to expand FISA to authorize warrants for physical searches it emphasized that the president already had independent constitutional power to do so.

As with all constitutional powers, the president may not authorize foreign intelligence surveillances that violate

the Fourth Amendment. But no serious person has suggested it is “unreasonable” for the government during a period of congressionally authorized war to intercept the communications of America’s enemies – and that need is arguably even *greater* when they are communicating with possible terrorists in this country. Congress may no more restrict the constitutional exercise of presidential discretion in this area than it could narrow the scope of the Fourth Amendment itself. And ultimate responsibility for balancing conflicting constitutional claims belongs to the Supreme Court, not the Congress.

Finally, we would do well to recall that FISA may have contributed to the FBI’s failure to prevent the 9/11 attacks. The reason “whistleblower” Colleen Rowley could not get a warrant to search the laptop of Zacarias Moussaoui prior to 9/11 was that Congress made no provision in FISA for surveillance of foreign terrorists who were not “agents” of a foreign power. At its core, her outrage was that the FBI’s national security lawyers had obeyed the law. It was not until 2004 that FISA was amended to address the “lone wolf” scenario.

America is a nation governed by the rule of law, and by all means we must ensure that no individual or institution in our government behaves to the contrary. But the primary “lawbreaking” in the present controversy was by *Congress*, and when statutes do battle with the Constitution they must properly and invariably *yield*. Sadly, much of the blame for the failure of our nation to understand these issues is directly attributable to a widespread ignorance about national security law.

Professor Turner holds both academic and professional doctorates from the University of Virginia School of Law, where in 1981 he co-founded the Center for National Security Law. He was a Senate staff member when FISA was first enacted and later oversaw its enforcement as Counsel to the President’s Intelligence Oversight Board in the White House. He chaired the Standing Committee between 1989 and 1992, edited this Report for the next seven years, and co-edits the casebook National Security Law. His testimony to the Senate Judiciary Committee on this issue may be found at: <http://www.virginia.edu/cnsl/>.

If the Commander in Chief Does It, It’s Not Illegal: The Nixon Doctrine Revived

David Cole

President Bush’s defense of his order authorizing the National Security Agency to spy on Americans without a warrant ultimately rests on a claim that Congress may not constitutionally limit the President’s authority, as Commander in Chief, to select the “means and methods of engaging the enemy.” This argument claims not only that the President has “inherent” power to collect “signals intelligence” on the enemy but that that inherent power cannot be regulated or checked by Congress – even when it includes wiretapping Americans in the United States without a warrant.

This claim of uncheckable or “exclusive” constitutional authority amounts to nothing less than a modified version of President Nixon’s infamous assertion that “when the President does it, that means that it is not illegal.” President Bush has revived that discredited doctrine, with only a slight modification: if the Commander in Chief does it, it is not illegal. This unprecedented assertion cannot be squared with our constitutional structure, which relies upon checks and balances. Moreover, the Supreme Court rejected the claim when President Bush’s lawyers made it in the Guantanamo detainees’ case, *Rasul v. Bush*, in 2004.

The President’s argument, articulated in a 42-page single-spaced memorandum submitted to Congress, is that the Commander in Chief has inherent power to select the “means and methods of engaging the enemy.” That power may not be restricted by Congress, the memo reasons. Since electronic surveillance related to al Qaeda falls within “engaging the enemy,” the president cannot be restricted in his decision to conduct such surveillance. Since detention and interrogation are also “means and methods of engaging the enemy,” it would follow that any congressional effort to regulate these matters is also unconstitutional.

The argument is nothing if not bold. But accepting it would require overturning the Supreme Court’s decision in *Rasul v. Bush*, the Guantanamo detainees’

Continued on page 10

Commander-in-Chief...

Continued from page 9

case. There, the Bush administration maintained that interpreting the habeas corpus statute to extend to enemy combatants held at Guantanamo “would directly interfere with the Executive’s conduct of the military campaign against al Qaeda and its supporters,” and would therefore raise “grave constitutional problems.” Rejecting this argument, the Court ruled that Congress had conferred habeas jurisdiction on the federal courts to entertain the detainees’ habeas actions. Even Justice Scalia, who dissented, agreed that Congress could have extended habeas jurisdiction to the Guantanamo detainees. Thus, not one member of the Supreme Court accepted the president’s Commander in Chief argument.

The administration’s defenders often protest that even if his NSA spying program violates a criminal statute, that does not make the program illegal because a statute cannot override the Constitution. Therefore, it is said, if the president could engage in foreign intelligence surveillance before Congress regulated that conduct in the Foreign Intelligence Surveillance Act (FISA), Congress cannot constitutionally limit his ability to do it thereafter. They then point to the fact that before FISA, presidents routinely conducted foreign intelligence surveillance, and that the Clinton administration itself asserted the president’s inherent authority to conduct physical searches for foreign intelligence purposes.

This argument reflects a fundamental misunderstanding of separation of powers doctrine. That doctrine holds that the President’s power to act is directly affected by actions taken by Congress. As Justice Robert Jackson explained in his influential opinion in *Youngstown Sheet & Tube Co. v. Sawyer*, a 1952 case invalidating President Truman’s seizure of steel mills during the Korean War, under our system of checks and balances, Congress’s actions are critical to assessing the scope of the President’s powers. When Congress has approved of the president’s actions, even implicitly the president’s powers are at their zenith; but when Congress has passed a law barring the President’s actions, he may act in contravention of that statute only if Congress is “disabled from acting” upon

the subject.

Before FISA was enacted, Congress had acknowledged by statute the President’s authority to engage in foreign intelligence, and his power was therefore at its fullest. When it enacted FISA, however, it repealed the earlier acknowledgment, and made it a crime to engage in wiretapping without statutory authorization. Similarly, President Clinton took the position that he could engage in warrantless physical searches only before FISA applied to physical searches; he then supported and signed the extension of FISA to physical searches, and could not have engaged in warrantless searches thereafter.

Can Congress limit the President’s “inherent” power in this setting? Congress plainly is not “disabled from acting” upon the subject of wiretapping of Americans. It has done so for years, and its authority to do stems directly from its authority over interstate and foreign commerce. Moreover, the Constitution gives Congress broad power to regulate the Commander in Chief’s conduct of a war. Congress defines the scope of the war under its power to declare war; it decides whether there shall be an army and how much it should be funded; and it creates rules and regulations to govern the army. It has long subjected the Commander in Chief to the Uniform Code of Military Justice, enacted statutes regarding the governance of occupied territories, extended habeas corpus to enemy combatant detainees, and prohibited torture and cruel, inhuman and degrading treatment. On the administration’s theory of an uncheckable Commander in Chief, all of these laws would be unconstitutional.

The Supreme Court has consistently rejected claims that the Commander in Chief can act contrary to statute, or cannot be checked by the other branches. In addition to the Guantanamo and steel seizure cases mentioned above, the Court in *Little v. Barreme*, an 1804 decision, ruled unlawful a presidentially ordered seizure 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.

And in *Hamdi v. Rumsfeld*, the Court expressly 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."

The fact that the Supreme Court has never found a Commander in Chief function that could not be regulated by Congress does not mean, of course, that there are no limits on Congress's power. If Congress sought to micromanage the war by assigning authority to lead the troops to someone outside the president's chain of command, for example, or if it sought to direct day-to-day battlefield strategy, its actions would likely be unconstitutional. But the notion that it cannot protect the privacy of Americans during wartime by requiring the president to obtain a warrant before spying on Americans is entirely unprecedented – unless, that is, you consider Richard Nixon a precedent.

David Cole is a Professor of Law at Georgetown University Law Center, the author of Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism, and the co-author of Terrorism and the Constitution: Sacrificing Civil Liberties for National Security. He is pro bono co-counsel in Center for Constitutional Rights v. Bush, which challenges the legality of the NSA spying program. A modified version of this essay appeared on Slate.com.

Above the Law?

Andrew C. McCarthy

There are three terribly disappointing things about the current controversy over President's wartime authorization of the National Security Agency to conduct warrantless surveillance of communications involving the enemy overseas which cross U.S. boundaries. The first is how politically polarized we are – such that the debate is much more a referendum about the Bush administration than about the quite distinct issue of presidential power. Second, perhaps of necessity, is

that our analytical prism is *legality* (a subordinate consideration in national security terms, but one the many complexities of which are grist for irreconcilable disagreement) rather than the far more consequential *practicality* (i.e., does the program really make us safer, something that probably cannot be known without compromising operational details).

Regrettably, this priority inversion is only added to, however marginally, by addressing the third difficulty, the subject of this essay, which is the issue's framing as whether the President has placed himself "above the law." This question is generally, and misleadingly, posed with the 1978 Foreign Intelligence Surveillance Act (FISA) as the frame of reference.

In point of fact, Congress frequently enacts laws that impinge on the prerogatives of other actors – whether individuals, states, courts, or the executive. But none of the latter imperiously puts itself "above the law" merely by the unremarkable happenstance of being at loggerheads with the legislature in a system the very basis of which is divided (and thus competing) powers. It is the Constitution, not the handiwork of Congress, that is the law for these purposes. And it is *that* law to which Congress, too, is subservient. Indeed, when a legislative enactment undermines the Constitution's structure, that is a case of *Congress*, if anyone, placing itself above the law.

Such loaded contentions, of course, generate much more heat than light. After all, Congress is rarely wholly off the reservation when it legislates, and the same can be said for virtually all presidential initiatives. There is almost always some legitimate prerogative catalyzing the actions of the political branches. It is part of the genius of our Constitution that the Framers did not define the ultimate boundaries of executive and legislative power. They gave us, instead, a flexible system, capable both of maximizing freedom and meeting threats. Both branches require the other's cooperation if they are to function at all, they have functions that overlap, and they collaborate or compete based on the circumstances.

The Framers also recognized (as the great political philosophers who influenced them had recognized) the

Continued on page 12

Above the Law...

Continued from page 11

difference in kind between the realms of domestic regulation and foreign affairs. The body politic is a consensual political community, in which government has a relative monopoly over the use of force, free citizens are vested with various rights and presumptions, and courts are interposed, in part, to inhibit executive overreach. In this domestic realm, Congress's enumerated powers are extensive and broad. Yes, the President has robust police powers, but no one could credibly contend that Congress acted illegitimately in imposing standards beyond the Fourth Amendment threshold for criminal wiretaps.

But the body politic's interactions with the rest of the world are another matter entirely. For all our sonorous rhetoric about an "international community," there is no global political unit. It's a jungle out there. Nations and factions (including transnational terror networks) all claim the right to use force – at times, existentially threatening force. The fluid, unstable circumstances are not sensibly given to antecedent, positive laws. And while our citizens are presumed innocent and entitled to privacy in our domestic courts, the presumption must favor government in the international sphere, where its failure against our enemies would endanger all of our civil liberties.

It was in this connection that the Framers created an energetic executive. Not simply one who would be commander-in-chief of the armed forces (the power most often highlighted in the current debate), but one in whom *all* executive power is vested, and on whom alone is imposed the duty to "preserve, protect, and defend the Constitution." The Supreme Court has thus long recognized, for example, the "delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations." At the core of that plenary power is the gathering of foreign intelligence – even in peacetime, let alone when our nation is at war against an enemy that has already catastrophically struck the homeland and makes no secret of its commitment to do so again, with the very real possibility of incalculable deadlines.

In the current debate, we are talking not merely about foreign intelligence but about the most ominous category of such intelligence: wartime communications crossing U.S. lines involving an enemy plotting to attack us

domestically. Were we able to fix the location from which al Qaeda operatives were calling into the United States, our military would need no judge's imprimatur to kill or capture them. The thought that the executive branch nonetheless needs a judicial warrant merely to listen to what is being said is anomalous to say the least.

An interpretation of FISA that would restrict the power of the President to design a foreign intelligence collection effort that is, in his judgment, necessary to create an early warning system against a (very likely) enemy attack would be unconstitutional. Congress unquestionably has the authority to prescribe rules for government, but it is not a limitless power, and it cannot reduce the core of presidential power created by the Constitution. Congress can declare war, and it can surely choose whether to fund wartime operations, effectively halting war if it so chooses. But it cannot conduct war. That is an executive function. The penetration of enemy communications is as rudimentary an aspect of war-fighting as deciding when to attack, which targets to hit, or what enemy operatives to detain.

Concern over executive actions that impinge on our liberties is always appropriate. If Congress believes the President has drawn the line improperly with the NSA program, it has its remedy – it can forthrightly defund the program. An informed electorate can then render its judgment at the ballot-box as to which resolution of the tension between liberty and security it prefers. That is how our constitutional democracy is supposed to work. Neither constitutional democracy nor national security is well served, though, by demagogic claims that the President has placed himself above the law.

Andrew McCarthy was an Assistant United States Attorney in the Southern District of New York from 1993 to 1996, during which time he led the prosecution of Sheik Omar Abdel Rahman and his followers in connection with the 1993 World Trade Center bombing and a conspiracy to attack other New York City landmarks. He is a recipient of the Attorney General's Exceptional Service Award and the Distinguished Service Award. He is currently a Senior Fellow with the Foundation for Defense of Democracies.

Understanding Counterterrorism Technology and Privacy

Richard E. Friedman

In drafting the Constitution, Benjamin Franklin and the other founders paid special attention to protection of civil liberties; they also provided that the federal government protect the nation against invasion. At that time, Franklin had no way of knowing that his 1752 kite experiment with the mysteries of electricity would lead to the computer age with super-computer capability and the ability to pinpoint many personal details of our daily lives. Today, there exists major tension between counterterrorism technology and the privacy guaranteed by the Fourth Amendment of the US Constitution, which is the subject of this essay.

There are passionate, reasonable arguments on both sides regarding the recent revelation of warrantless, electronic eavesdropping on suspected terrorists. Recent revelations that a blogger purchased the cellphone records of a 2004 presidential candidate for less than \$100 sounds a warning about privacy, secrecy, and anonymity. A cellphone was a novelty less than 10 years ago. It is likely that new, innovative uses of computers will continue to expand.

Recent revelations of presidential authorization of electronic surveillance of US persons within the US without a warrant or court order serve to frame a critical strategic issue: how to keep the US safe from catastrophic terrorism incidents while protecting citizens' right to privacy.

The warrantless wiretap matter floats on conjecture and speculation. Many of the facts are unknown. There are complex legal issues embedded, such as the jurisdictional scope of the Foreign Surveillance Intelligence Act (FISA), the limits of presidential power under Article II of the Constitution, and the unresolved conflict between the executive and legislative branches of government regarding primacy in time of war. Cogent arguments will be advanced on these issues, and they may have to be resolved by the US Supreme Court.

Counterterrorism technology and privacy is a critically important strategic issue. This subject was addressed in June, 2004 at a conference organized and conducted by the National Strategy Forum and the American Bar Association Standing Committee on Law and National

Security, and underwritten by the McCormick Tribune Foundation as part of their Cantigny conference series. The following observations are drawn largely from the balanced discussion at that conference. The post-conference report may be accessed via the NSF website, www.nationalstrategy.com.

Information technology is a critical counterterrorism tool. Technology permits government and business to collect, store, analyze, and disseminate an enormous amount of information about how we conduct our daily lives. This information is collected and stored primarily by commercial entities and, to a lesser extent, by government. Computers can be used to correlate information from multiple databases. Today, technology exists that can identify one's shoe size, style preference, place purchased, and the presence of athlete's foot. The expense of collecting and storing this data is constantly decreasing.

Our society is ambivalent, or strongly opposed, to the use of information technology because of personal privacy concerns. The expectation of privacy that existed a mere 30 years ago is gone. We know, for example, that credit card transactions will become part of a commercial database. This constitutes a voluntary surrender of personal information—a tradeoff between convenience and personal privacy.

Society has a legitimate interest in identifying sexual predators who prey on children, which is a crime in all jurisdictions. A law enforcement investigator will look for a known sex offender in the vicinity of the crime using “street informants,” credit card transactions, and phone records. The positive result could be a successful prosecution of the offender after the crime has been committed. Counterterrorism is a reverse of this process. Counterterrorism involves deterrence and prevention—the objective is to intercept and neutralize terrorists who have not yet committed an act of terrorism.

The federal government is responsible for deterring and preventing a catastrophic terrorism incident. To that end, it relies on counterterrorism technology. The law enforcement and counterterrorism communities deal with the same information, but for different purposes and use different methodologies. Law enforcement begins with a focus on an individual; counterterrorism looks for patterns that lead to individuals or groups of individuals. The common source used by law

enforcement and counterterrorism investigators is a universe of information – a “mine.” The methodology used to distill and synthesize information is “data mining.” The nuggets of information in the mine are composed of bits of information derived from the daily, mundane activities of law-abiding citizens and the intermittent actions of bad guys.

Three different concepts are in play: privacy, secrecy, and anonymity. In contemporary society anonymity has largely disappeared. Moreover, personal privacy has been vastly diminished in the past two decades and will continue to diminish in the future. The rationale for this contention is that, if one uses a telephone or credit card, we have tacitly accepted a high degree of intrusion on our privacy. If personal privacy has already been greatly reduced, the concern shifts to notions of secrecy and how to prevent government from abusing what is deemed to be personal secrecy.

So, we have the interests of individuals and their desire for privacy, and the interests of the government to protect society by preventing acts of terrorism. To do this, the government must “connect the dots” to identify bits of relevant information and to perceive patterns of behavior. To achieve this, vast amounts of information are collected, arrayed, sorted, collated, and ultimately used or ignored. There is general agreement that most information is rejected and never surfaces.

There is a strong contra-argument that the mere act of government acquiring personal information is a denial of civil liberties. Another civil liberties concern is that data mining for terrorist activity may uncover non-terrorist-related criminal activity, major or minor criminal offenses that in the normal course of events would not have been discovered without a search warrant as required by the Fourth Amendment. The US Centers for Disease Control routinely uses data mining techniques, without warrants, to determine the source of an epidemic or pandemic, notwithstanding stringent personal health privacy laws. This practice has been met with negligible objection. Yet, there is public outcry when the government uses similar methodologies for counterterrorism purposes.

Expectations of privacy are in imminent jeopardy of being eroded by new technology. The discussion may shift away from abstract discussion towards concrete rules designed to protect privacy. However, technology-specific legislation may not be the answer because

it is likely that rapid advances in technology will outpace, bypass, and invalidate even the most balanced and farsighted legislation.

Technology provides neither total security nor total privacy. Technology is neutral. It is part of a system that can be used to protect personal security – to protect citizens from a catastrophic terrorism incident or a suicide bomber wreaking havoc at a wedding reception. A second value is that a reasonable policy, one that is widely supported by the public, will effectively manage the technical system to conform to another value, which is protection of civil liberties. The goal is a policy that balances government’s and society’s need for information, with personal needs for protection against surveillance.

The meaning of personal privacy these days is dynamic and, to some degree, imprecise. A new era of uncertainty has arrived. One approach is to attempt to restrict the development of new technology and severely limit its use. However, for better or worse, the barn door is open. Thus, the debate shifts to the abuse of technology. The Cantigny conference on Counterterrorism Technology and Privacy reached no conclusion, but it outlined the elements of a strategy.

- Clear legal limits on the uses of data mining and related technology.
- Clear and understandable oversight mechanisms.
- An open process allowing for the participation of interest groups.
- Mechanisms for the redress of grievances for those who may have been adversely affected by the application of the technology.
- Positive explanations of technological proposals to the public and press.
- Restraint in public statements (i.e., using care in communications and restraining the urge to over-promise or over-criticize).

Civil liberties concerns include:

- Existing laws do not regulate the government’s use of commercial data for counterterrorism purposes.
- The purposes of law enforcement and counterterrorism.
- How is personal information being collected and used? What appropriate safeguards are in place?
- The need for effective Congressional oversight and government agency accountability.
- Does the mere viewing of personal records – even if there are no consequences from the inspection –

constitute an invasion of privacy? (Profiling and focus on people of the Islamic faith are examples.)

- Transparency of government data collection and methodology.
- In the event of misidentification of an individual, is there adequate redress?

Virtually all Americans want to be secure, personally and nationally. But we also cherish the civil liberties found in the US Constitution. It is important for all Americans to be informed and to understand legitimate

concerns regarding actual and potential incursions into civil liberties – “trampling on civil liberties”. This requires critical evaluation and civil discussion among all parties to reach a conclusion on a complex and vital issue.

Richard Friedman is the President and Chair of the National Strategy Forum and Chair of the Advisory Committee of the American Bar Association Standing Committee on Law and National Security.

Additional Resources Concerning the NSA Surveillance Debate

- December 22, 2005: Letter from Assistant Attorney General William Moschella (Office of Legislative Affairs) to Senators Roberts and Rockefeller and Representatives Hoekstra and Harman, providing a five-page summary of the legal authority for warrantless NSA surveillance activities (<http://www.washingtonpost.com/wp-srv/politics/documents/122205NSAletter.pdf>).
- January 5, 2006: Elizabeth B. Bazan and Jennifer K. Elsea, Congressional Research Service, “Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information” (<http://www.fas.org/sgp/crs/intel/m010506.pdf>).
- January 9, 2006: Letter to Congressional leadership criticizing the legality of the NSA program, by Curtis A. Bradley, David Cole, Walter Dellinger, Ronald Dworkin, Richard Epstein, Harold Hongju Koh, Philip B. Heymann, Martin S. Lederman, Beth Nolan, William S. Sessions, Geoffrey R. Stone, Kathleen M. Sullivan, Laurence H. Tribe, and William W. Van Alstyne (<http://cdt.org/security/20060109legalexpertanalysis.pdf>).
- January 19, 2006: Justice Department “White Paper” defending the legality of the NSA program (<http://news.findlaw.com/hdocs/docs/nsa/dojnsa11906wp.pdf>), and accompanying cover letter from Attorney General Alberto Gonzales to Senate Majority Leader Frist (<http://news.findlaw.com/hdocs/docs/nsa/dojnsa11906ltr.pdf>).
- January 24 2006: Remarks by Attorney General Alberto Gonzales defending the legality of the NSA program, delivered at Georgetown (http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html).
- February 6, 2006: Senate Judiciary Committee, Testimony from Attorney General Alberto Gonzales (<http://judiciary.senate.gov/hearing.cfm?id=1727>).
- February 28, 2006: Senate Judiciary Committee, Testimony from James Woolsey, Harold Hongju Koh, Ken Gormley, Douglas Kmiec, Bruce Fein, Robert Turner, and Robert Levy (<http://judiciary.senate.gov/hearing.cfm?id=1770>).
- February 28, 2006: Letter from Attorney General Alberto Gonzales to Senator Arlen Specter, supplementing and clarifying responses from the February 6, 2006 hearing (<http://www.washingtonpost.com/wp-srv/nation/nationalsecurity/gonzales.letter.pdf>).

In Case You Missed It ...

Staying current in the field of national security law is never easy. Every week there are significant new opinions, statutes, indictments, reports, articles, and any number of other developments. Many of these items prompt coverage in the major media outlets, but some fly beneath the radar. In an effort to assist practitioners and scholars in keeping up to date with these events – and in particular to provide ready access to primary sources in electronic format – Professor Robert Chesney of Wake Forest University School of Law maintains a listserv for professionals and academics working in this area. “In Case You Missed It...,” featuring selected posts from that listserv, will be a recurring item on the back page of the National Security Law Report. Those interested in subscribing to the listserv may do so by contacting Professor Chesney at rchesney@law.wfu.edu.

-
- In late March the Supreme Court will hear oral argument in *Hamdan v. Rumsfeld*, No. 05-184, concerning a challenge to the legality of the military commission process and also presenting questions concerning the impact of the recently enacted Detainee Treatment Act of 2005. A convenient collection of the briefs in *Hamdan* is posted here: <http://www.hamdanvrumfeld.com/briefs>.
 - The White House report on the response to Hurricane Katrina is posted here: <http://www.whitehouse.gov/reports/katrina-lessons-learned/>.
The House Select Committee report on the response to Hurricane Katrina is posted here: <http://katrina.house.gov/>.
 - *United States v. Amawi, et al.* (N.D. Ohio Feb. 16, 2006) (indictment). A grand jury in Ohio has indicted three individuals for their alleged involvement in a conspiracy to travel to Iraq to carry out attacks against U.S. forces there, and to put together a recruiting, funding, and training system for that purpose. The indictment is posted here: <http://news.findlaw.com/hdocs/docs/terrorism/usamawai21606ind.html>.
 - *Arar v. Ashcroft*, No. cv-04-249 (E.D.N.Y. Feb. 16, 2006) (dismissing the civil suit brought by Maher Arar against John Ashcroft and others in connection with the rendition of Arar from JFK Airport to Syria in October 2002). The opinion is posted here: http://www.ccr-ny.org/v2/legal/september_11th/docs/Arar_Order_21606.pdf.
 - *Omar v. Harvey*, No. 05-2347 (D.D.C. Feb. 14, 2006) (preliminary injunction) (prohibiting U.S. military from transferring petitioner – a U.S. citizen held in Iraq under the auspices of the Multi-National Force-Iraq – to the custody of the Iraqi government)
 - *United States v. Assi*, 2006 WL 335891 (E.D. Mich. Feb. 10, 2006) (upholding constitutionality of 18 USC § 2339B, the law prohibiting material support to designated foreign terrorist organizations).
 - Completion of Administrative Review Board Proceedings for Guantanamo Bay detainees: <http://www.defenselink.mil/releases/2006/nr20060209-12464.html>.
 - Release of hearing transcripts from Combatant Status Review Tribunals at Guantanamo Bay: <http://www.defenselink.mil/pubs/foi/detainees/csrt/index.html>.
 - *United States v. Khadr* (D. Mass. Feb. 6, 2006) (indictment). A grand jury has indicted Abdullah Ahmed Khadr on charges involving a plot to carry out attacks on U.S. and allied forces operating near the Afghan/Pakistan border. The indictment is posted here: <http://news.findlaw.com/hdocs/docs/terrorism/uskhadr20706ind.html>.
-