HARVARD UNIVERSITY
Hauser Hall 420
Cambridge, Massachusetts 02138
tribe@law.harvard.edu

Laurence H. Tribe
Carl M. Loeb University Professor

Tel.: 617-495-4621
Fax: 617-495-3383

January 6, 2006

The Honorable Michael E. Capuano.
United States House of Representatives
1530 Longworth House Office Bldg.
Washington, DC 20515-2108

Dear Congressman Capuano:

I appreciate your interest in my views as a constitutional scholar regarding the legality of the classified program of electronic surveillance by the National Security Agency ("NSA") that the President authorized within months of the September 11, 2001, attacks by Al Qaeda, a program whose existence the President confirmed on December 17, 2005, following its disclosure by *The New York Times* several days earlier.

Some have defended the NSA program as though it involved nothing beyond computer-enhanced data mining used to trace the electronic paths followed by phone calls and e-mails either originating from or terminating at points overseas associated with terrorists or their affiliates or supporters. But that type of intelligence gathering, whose history long antedates September 11, 2001, typically entails little or no interception of communicative *content* that would make it a "search" or "seizure" as those terms are understood for Fourth Amendment purposes (see *Smith v. Maryland,* 442 U.S. 735 (1979) (the "pen register" case)), or "electronic surveillance" as that term is used in the Foreign Intelligence Surveillance Act (FISA)(see 50 U.S.C. § 1801 (f)(1)-(2)). Unfortunately, as Attorney General Gonzales candidly conceded in a press briefing on December 19, 2005, the program under discussion here authorized *precisely* such interception of "contents of communications." See http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html.

Although there may be room for debate about the boundary between content interception and mere traffic analysis in other contexts, the Attorney General eliminated speculation on the point when he said in that press briefing 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," and it is undisputed that a court order is precisely what the Executive Branch chose to proceed *without*. The President was therefore being less than forthright when, two weeks after

admitting that he had authorized what the FISA defines as "electronic surveillance" that would normally require a judicial warrant, he told reporters in Texas that the "NSA program is one that *listens to a few numbers*" because "the enemy is calling somebody and we want to know *who they're calling* . . . ." See http://www.nytimes.com/aponline/national/AP-Bush.html?ei=5094&en=8b73b4903455b75... (1/3/2006). To be sure, the President did say "we want to know who they're calling *and why," to* "find out what the enemy's *thinking,"* hopefully alerting the attentive listener to the possibility that the contents of individual messages are being intercepted. But by centering the discussion on what sounds more like number-crunching than content-trawling, the President encouraged the program's other apologists to depict it as relatively innocuous by shifting attention away from precisely what makes this program of secret surveillance so legally controversial.

Equally diversionary is the frequently repeated suggestion that, whatever the program intercepts, the only messages it reaches are "communications, back and forth, from within the United States to overseas *with members of Al Qaeda*," to quote the Attorney General's December 19 press briefing. Again, however, the attentive listener might have caught the more precise account the Attorney General let slip at another point in that same briefing, when he noted that the surveillance that had been going on under presidential auspices for roughly four years in fact reaches all instances in which "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." Given the breadth and elasticity of the notions of "affiliation" and "support," coupled with the loosely-knit network of groups that Al Qaeda is thought to have become, that definition casts so wide a net that no-one can feel certain of escaping its grasp.

A strong case can be made that, even under the circumstances confronting the United States in the aftermath of the terrorist attacks launched by Al Qaeda on September 11, 2001, and even with assurance that conversations are being intercepted solely to aid in preventing future terrorist attacks rather than for use as evidence to prosecute past misdeeds, so indiscriminate and sweeping a scheme of domestic intrusion into the private communications of American citizens, predicated entirely on the unchecked judgment of the Executive Branch, violates the Fourth Amendment "right of the people to be secure . . . against unreasonable searches and seizures" even if it otherwise represents an exercise of constitutional power entrusted to the President by Article II or delegated to the President by Congress in exercising its powers under Article I.

The precise question of such a scheme's consistency with the Fourth Amendment has never been judicially resolved — nor is it likely to be resolved in this situation. For the scheme in question, far from being *authorized* by Congress, flies in the face of an *explicit congressional prohibition* and is therefore unconstitutional without regard to the Fourth Amendment unless it belongs to that truly rare species of executive acts so central to and inherent in the power vested in the President by Article II that, like the power to propose or veto legislation or to issue pardons, its exercise cannot constitutionally be fettered in any way by the Legislative Branch.

Any such characterization would be hard to take seriously with respect to unchecked warrantless wiretapping. As the Supreme Court famously held in *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579 (1952), an emergency presidential takeover for a limited time of certain critical publicly held corporations like Bethlehem Steele Co. and the United States Steele Co., in order to avert the threat that would be posed to our national security by a stoppage of the steel production needed for weapons and other materials essential to the ongoing Korean War, falls outside that tiny category of congressionally illimitable executive acts and is indeed unconstitutional unless affirmatively authorized by Congress. If that is so, then certainly an unchecked presidential program of secretly recording the conversations of perhaps thousands of innocent private citizens in the United States in hopes of gathering intelligence potentially useful for the ongoing war on a global terrorist network not only falls outside that category but misses it by a mile.

The only escape from that conclusion would be to hold that inherent and illimitable presidential power to abridge individual liberty and erode personal privacy categorically exceeds presidential power to displace temporarily the corporate managers of entirely impersonal business property, without confiscating, transferring, or otherwise touching the property's ultimate ownership by the holders of its shares. But our Constitution embodies no such perverse system of priorities.

The presidential power at issue in this case is therefore subject to the control of Congress. And that Congress has indeed forbidden this exercise of power is clear. The Foreign Intelligence Surveillance Act of 1978 unambiguously limits warrantless domestic electronic surveillance, *even in a congressionally declared war*, to the first 15 days of that war; criminalizes any such electronic surveillance not authorized by statute; and expressly establishes FISA and two chapters of the federal criminal code, governing wiretaps for intelligence purposes and for criminal investigation, respectively, as the "*exclusive* means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 50 U.S.C. §§ 1811, 1809, 18 U.S.C. § 2511(2)(f). The House version of the bill would have authorized the President to engage in warrantless electronic surveillance for the *first year* of a war, but the Conference Committee rejected so long a period of judicially unchecked eavesdropping as unnecessary inasmuch as the 15-day period would "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). If a year was deemed too long, one can just imagine what the Conferees would have said of *four* years.

Rather than reaching for the heaviest (and, in this context, least plausible and hence most ineffectual) artillery by claiming an inherent presidential power to spy on innocent American citizens within the United States even in the teeth of a clear and explicit congressional prohibition of that technique of intelligence-gathering beyond the first 15 days of a declared war, the administration points to the FISA's own caveat that its prohibitions are inapplicable to electronic surveillance that is "otherwise authorized" by a congressional statute, which of course encompasses a joint resolution presented to and signed by the President.

The Authorization to Use Military Force (AUMF) against Al Qaeda, Pub.L. No. 107-40, 115 Stat. 224 §2 (a) (2001), is just such a resolution, the administration claims, for it 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 aggression. Although that resolution of course says nothing about electronic surveillance as such, neither does it say anything specifically about the detention of enemy combatants fighting for Al Qaeda in Afghanistan as part of the Taliban, the organization from within which the Al Qaeda terrorist network launched those infamous attacks. Yet, in the face of congressional legislation (the Non-Detention Act) expressly forbidding the executive detention of any United States citizen except "pursuant to an Act of Congress," 18 U.S.C. § 4001(a), the Supreme Court in *Hamdi v. Rumsfeld,* 124 S.Ct. 2633 (2004), held that such detention in the United States of individuals who are U.S. citizens captured while fighting against American forces in Afghanistan "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," escapes the prohibition of that anti-detention statute by virtue of its implied authorization by the AUMF as an exercise of the "necessary and appropriate force" Congress authorized the President to use, a conclusion supported by the fact that such detention for this limited purpose is a "fundamental and accepted . . . incident to war." 124 S.Ct. at 2640.

If *Hamdi* treated the AUMF as an "explicit congressional authorization," 124 S.Ct. at 2640-41, for *imprisoning* an enemy combatant despite AUMF's failure to mention "detention" or "imprisonment" in so many words, the argument goes, the AUMF must be read to impliedly authorize the far less severe intrusion of merely *eavesdropping* on our terrorist enemies, and on members of organizations that indirectly support them. After all, the collection of "signals intelligence" about our enemies abroad is no less an accepted incident of war than detaining the captured enemy — just as signals intelligence of foreign agents (including some going to and from the United States) has been accepted as an inherent power of the President even in the *absence* of war. Surely, then, now that Al Qaeda *has* launched a war against us, and now that Congress has responded with the functional equivalent of a declaration of war in the AUMF, even the entirely innocent American citizen in Chicago or Cleveland whose phone conversation with a member of an Al Qaeda-supportive organization happens to be ensnared by the eavesdropping being undertaken by the NSA cannot be heard to complain that no statute specifically authorized the Executive to capture her telephone communications and e-mails as such. Invasion of that citizen's privacy was, alas, but one of war's sad side effects — a species of collateral damage.

The technical legal term for that, I believe, is poppycock. *Hamdi* obviously rested on the modest point that statutory authority to kill or gravely injure an enemy on the field of battle impliedly authorizes one to take the far less extreme step of detaining that enemy, solely for the duration of the battle, to prevent his return to fight against our troops. Power to engage in domestic electronic surveillance on a wide scale within the territorial United States — intercepting, recording and transcribing conversations of

unsuspecting citizens who have committed no wrong, are not foreign agents traveling to and from the United States, and in fact pose no threat themselves but merely happen to have accepted a phone call or received an e-mail from, or sent an e-mail to, a member of an organization that is said to be supportive of the Al Qaeda network — is by no stretch of the legal imagination a "lesser included power" contained within the power to repel future terrorist attacks by Al Qaeda on the United States.

Thus the argument that the AUMF does not impliedly authorize this wide-ranging and indefinitely enduring program to extract potentially useful intelligence from ordinary citizens easily survives challenge based on *Hamdi*. More than that, *Hamdi* in fact yields added *support* for the conclusion that the AUMF cannot provide the requisite authorization. For the *Hamdi* plurality agreed "that *indefinite* detention *for the purpose of interrogation,*" even of conceded enemy combatants, "is not authorized" by the AUMF. 124 S.Ct. at 2641 (emphasis added). It follows *a fortiori* that indefinite subjection of American citizens who are not even *alleged* to be enemies, much less enemy *combatants*, to ongoing invasions of their privacy in the United States for purposes of obtaining valuable information is not authorized either.

Moreover, it makes a difference that the FISA's specific regulation of all electronic surveillance in the United States deals with the subject at issue here in a far more comprehensive and elaborate way than the Anti-Detention Statute involved in *Hamdi* dealt with the military detentions at issue there — military detentions that the Court treated as falling within the Anti-Detention Statute merely for the sake of argument when it held only that, *if* that statute otherwise applied, then it was trumped by the more specifically relevant AUMF. Here, in contrast, there can be no serious doubt that it is the FISA, and not the AUMF, that deals more specifically with the activity in question.

Construing the AUMF, taken in conjunction with the President's power as Commander in Chief under Article II, as implicitly conferring broad authority to engage in whatever warrantless surveillance the President might deem necessary in a war of indefinite duration against Al Qaeda-related terrorism even in the face of FISA's prohibitions would entail interpreting the AUMF far more broadly than anyone could, in truth, have anticipated. If that AUMF authorization were indeed *this* broad, the President must simply have overlooked its continued existence when he recently chided Congress for failing to reenact the PATRIOT Act's provisions. To be sure, the AUMF, even on the Justice Department's extravagant reading, enacted no *criminal* proscriptions of the sort that parts of the PATRIOT Act included. Nor did it purport to authorize the President to enact such criminal laws, morphing into some sort of one-man legislature. But, on the government's broad reading, the AUMF certainly *had* armed the President, as of September 18, 2001, with the authority to take most of the steps the PATRIOT Act expressly authorized — including *all* of the purely investigative and preventive actions it empowered the President to take — until the recent sunsetting of some of its provisions. And it had empowered him as well, again on the government's reading, to override any statutory prohibitions that might otherwise have stood in his way.

On the government's proposed reading of the AUMF, in other words, the PATRIOT Act, insofar as it confers the powers of investigation and prevention most fiercely sought by the President, becomes a needless and mostly redundant bauble. A statutory construction with such bizarre and altogether unanticipated consequences — and one that rests on so shaky a foundation — would be inadmissible even if accepting it would not leave us with serious questions under the Fourth Amendment, which it of course would.

Finally, it is telling that Attorney General Gonzales, when asked in his December 19 press briefing why the administration hadn't simply proposed to Congress, in closed session if necessary, that it amend FISA to grant legislative permission for the kind of domestic surveillance program the President deemed essential to the nation's security, replied that the administration had concluded such a request would probably have been futile because Congress would most likely have denied the authority sought! To argue that one *couldn't have gotten* congressional authorization (in late 2001, when the NSA program was secretly launched) after arguing that, by the way, one *did* get congressional authorization (in late 2001, when the AUMF was enacted) takes some nerve. Apart from the obvious lapse in logic, it is axiomatic that legislative reluctance to relax or eliminate a prohibition is no defense to a charge of its violation.

The inescapable conclusion is that the AUMF did *not* implicitly authorize what the FISA expressly prohibited. It follows that the presidential program of surveillance at issue here is a violation of the separation of powers — as grave an abuse of executive authority as I can recall ever having studied.

Yours truly,

Laurence H. Tribe