

Honorable Nancy Pelosi
United States House of Representatives
Washington, D.C. 20515-0508

Senate Majority Leader Harry Reid
United States Senate
Washington, D.C. 20510-2803

September 4, 2007

Dear Speaker Pelosi and Leader Reid,

We are organizations that believe that our nation's surveillance laws can effectively target terrorists without jeopardizing the rights of innocent United States persons. We are very concerned that the recently enacted Protect America Act of 2007 may be used to justify the warrantless interception of any international communications by U.S. persons without any restriction on the subsequent review and data mining of the metadata concerning those calls or the content of the communications themselves.

We are encouraged by your requests to the Judiciary and Intelligence Committees to once again delve into the Foreign Intelligence Surveillance Act (FISA) and reinsert much needed privacy protections that were lacking in the last iteration. It stands to reason that just as the level of intrusion into U.S. persons' communications is dramatically increased, so too must be the protections for those communications. To that end, we would like to share basic principles that must be respected to ensure that U.S. persons' electronic communications are protected from unwarranted government intrusion:

1. No amendments to FISA should be made permanent until Congress and the public receive answers about what surveillance activities have been conducted over the last six years and the legal basis for those programs. Further, information regarding how the authorities provided for in the Protect America Act are being interpreted and operationalized by the National Security Agency should be shared with Congress. To facilitate Congress' legislative efforts, the NSA should be required to articulate with specificity the problematic aspects of the prior statutory scheme and whether the Protect America Act responds to those intelligence concerns.
2. Any further legislation must reiterate that FISA is the exclusive means of intelligence gathering on U.S. soil, and the legislation must include automatically triggered consequences for violating this exclusivity. As initially enacted by Congress, the exclusivity of FISA was unambiguous. This new exercise in defining the lawful extent of surveillance authorities will be useless if the resulting legislation can be ignored. We further recommend that any new legislation state explicitly that

the Authorization for the Use of Military Force in Afghanistan and Iraq do not authorize any surveillance outside FISA. Additionally, we recommend that the NSA be required to report to Congress repeatedly on its implementation of any new surveillance activities conducted pursuant to FISA.

3. Interceptions of U.S. persons' communications within the U.S. should continue to be included within, and, therefore, protected by the definition of "electronic surveillance." The Protect America Act's seeming elimination of this protection should be repealed.

4. Collection and isolation of the particular communications sought by the government should be conducted by the telecommunications industry itself – the government should not be given direct and unfettered access to telecommunications infrastructure. We are concerned that the PAA appears to allow the government to "sit on the line" and scoop up all communications and sort through them later. Instead, the government should receive only the information it is authorized to intercept by law.

5. The Foreign Intelligence Surveillance Court (FISC) must play a meaningful role in ensuring compliance with the law. First and foremost, electronic surveillance should be authorized by the FISC through the issuance of an individualized warrant based on probable cause. This oversight should include, where possible, prior and, always, regular judicial approval and review of surveillance based on full disclosure about what information is to be sought, whose communications will be collected, how it will be gathered and how content and other data in communications to and from the United States will be handled. The Court must also have regular access to information about how many U.S. communications are being collected and the authority to require court orders when it becomes clear that a certain program or surveillance of a target is scooping up communications of U.S. persons.

6. Under any new amendment to FISA established in your legislation, when the government intercepts a communication to which a person in the U.S. is a party, there should be a presumption requiring the NSA to immediately destroy that communication unless the NSA documents that it has reason to believe that the communication reflects an immediate threat to life or limb. Additionally, where the government has probable cause to believe communications into or out of the United States involve the planning for an international terrorist attack or an imminent hostile action by a foreign power, the government may keep and utilize the communication intercepted if the NSA documents their basis for that reasonable belief and subsequently applies for a warrant for that communication within 72 hours of its acquisition. The FISC may respond to such an application in one of three ways: (i) grant the order for the warrant to obtain retrospective and prospective approval to

monitor communications with that U.S. person and permit the NSA to utilize the communication; (ii) reject the order and require destruction of the U.S. person's communications intercepted; or (iii) extend the period under which this emergency period of interception may occur but require the re-filing of a revised warrant application within 72 hours. All public FISA legislation has been deficient in that it has lacked a presumption of destruction of the improperly intercepted communications of U.S. persons. Without such a presumption, the Administration's secret "minimization" procedures will be all that govern U.S. communications. Congress has the authority – and the responsibility – to explicitly define how these communications are treated, and should no longer defer to the Executive branch's unknown policies. If the programs are truly directed at people overseas, this should be noncontroversial. In the situation where the government obtains a communication with a U.S. person that suggests an attack by international terrorists is being planned or that a foreign power may take imminent hostile against the U.S., the new statutory regime would give flexibility to the NSA to protect the national security of the U.S., but not negatively impact the rights of U.S. persons without court supervision.

7. Once the government has reason to believe that there is a substantial likelihood that a specific account, person or facility will have contact with someone in the United States, the government should be required to return to the FISC to obtain a court order for continued surveillance of that account, person or facility. Reliance on the FISC will help ensure the privacy of U.S. persons' communications.

We are happy to discuss more precise language to effectuate these changes. We understand that the Administration's original intent was to allow easier collection of communications of people abroad that are incidentally routed through the United States. We look forward to working with you and the Committees to rein in this limitless program and devise one that actually gives the government access to these communications without jeopardizing the rights of people in the United States.

Sincerely,

Cc: Chairman Reyes, Ranking Member Hoekstra, Chairman Conyers, Ranking Member Smith