BARRY M. KAMINS
PRESIDENT
Phone: (212) 382-6700
Fax: (212) 768-8116
bkamins@nycbar.org

November 6, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Arlen Specter
Ranking Minority Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senators Leahy and Specter:

I write on behalf of the Association of the Bar of the City of New York ("the Association") to express the Association's strong opposition to the FISA Amendments Act of 2007 introduced by Senator Rockefeller and approved by the Select Committee on Intelligence, which is now pending before the Judiciary Committee. The FISA Amendments Act is intended to replace the Protect America Act hastily passed by Congress in August, but contains many of the same fundamental flaws, including (a) delegation to the Attorney General ("AG") and Director of National Intelligence ("DNI") of the authority to conduct warrantless surveillance on their own certification, without advance judicial approval; (b) the absence of meaningful judicial review by the FISA Court over the exercise of this authority by the AG and DNI; (c) the removal of warrantless surveillance directed at individuals reasonably believed to be overseas from the definition of "electronic surveillance" under FISA, and thus from the protections of the Act; and (d) the grant of authority to the AG and DNI to issue directives to communications service providers demanding compliance with a surveillance request, rather than requiring a court order to direct compliance. In addition, there is no legitimate basis for the provisions of the proposed FISA Amendments Act granting full immunity to communications service providers for their past cooperation with potentially unlawful surveillance requests, and the lengthy six-year sunset provision of the bill allows far too much time to elapse before requiring Congress to reevaluate whether there is a continuing need for the extraordinary authority granted by the bill.

The Association has endorsed, as an acceptable compromise, the proposed RESTORE Act (H.R. 3773) introduced in the House of Representatives by Chairman John Conyers, Jr. of the House Judiciary Committee and Chairman Silvestre Reyes of the House Committee on Intelligence. A copy of my October 16, 2007 letter to Speaker Nancy Pelosi setting out the Association's position on the

RESTORE Act and on another bill pending in the House, the proposed FISA Modernization Act (H.R. 3782) introduced by Congressman Rush Holt, is enclosed for your information. As discussed in my October 16 letter, the Association views the proposed Modernization Act as the preferable bill, because it more carefully defines the exclusion from FISA necessary to accommodate an exception for foreign-to-foreign communications, and would require individualized FISA warrants before permitting the interception of electronic communications between citizens and residents in the United States and individuals overseas. While the proposed RESTORE Act does not require individualized FISA warrants before interception of such international communications, the Association could support that bill as a compromise because it at least requires advance FISA Court approval of the Administration's foreign surveillance plans, as well as extensive oversight of the manner in which the Administration's surveillance program is being carried out.

In contrast, the Association views the proposed FISA Amendments Act as completely unacceptable in its present form, and urges the Judiciary Committee, and the Senate, to reject it unless it is amended substantially. As noted above, there are many fundamental flaws in the FISA Amendments Act, as a result of which the proposed Act fails to give adequate protection to the privacy interests of American citizens and residents and the confidentiality of their international communications.

First, the proposed Act does not require any advance judicial approval before permitting the AG and DNI to initiate surveillance of persons believed to be outside the United States, including their communications with persons inside the United States.[1] Proposed Section 703 would give the AG and DNI authority to jointly authorize the targeting of individuals reasonably believed to be outside the United States. Rather than require advance judicial approval, however, Section 703 merely requires the AG and DNI to prepare and ultimately file with the FISA Court a certification attesting that there are reasonable targeting procedures and minimization procedures in place which have been approved by, or will "promptly" be submitted for approval to, the Court; that the targeting procedures are, in their judgment, consistent with the Fourth Amendment; and that the surveillance is not intentionally targeting someone located in the United States. *See* Proposed Sections 703(d) – 703(g).[2]

---

[1] The Association has no objection to the provisions of the RESTORE Act which would permit the AG and DNI to authorize electronic surveillance of persons reasonably believed to be outside the United States, without seeking advance FISA court approval, in emergency situations. *See* RESTORE Act, Proposed FISA Section 105C. The FISA Amendments Act, however, would allow the AG and DNI to authorize warrantless surveillance on their own certification in all cases, whether or not there was an emergency.

[2] It should be noted, however, that the proposed FISA Amendments Act, as reported out of the Select Committee on Intelligence, includes a provision (proposed Section 703(c)) that would provide for substantially enhanced safeguards with respect to surveillance directed at United States persons overseas. Proposed Section 703(c) would require a FISA Court order before the Administration could target the communications of a United States person outside the United States, and also would require advance FISA Court approval of the procedures to be employed by the Administration in determining whether a proposed target overseas is in fact a United States person. *See* Proposed Section 703(c)(3). These provisions provide important additional protections for United States persons overseas, consistent with Fourth Amendment requirements, and should be preserved in the final version of the bill if the FISA Amendments Act goes forward.

Second, the proposed Act does not provide for adequate judicial review by the FISA Court of the actions taken by the AG and DNI. While the Act does include provisions for judicial review, these provisions are flawed and do not include meaningful judicial review of the most important aspects of the AG's and DNI's exercise of authority. The proposed Act provides for judicial review of the targeting and minimization procedures adopted by the Administration, but only to assess whether those procedures formally meet the statutory requirements, not to assess how those procedures are in fact being implemented. *See* Proposed Act Section 703(i)(3), (4).[3] Equally important, there is no substantive judicial review at all with respect to the rest of the AG's and DNI's certification; rather, the Act provides that the FISA Court's only role is to determine whether the certification "contains all the required elements." *See* Proposed Section 703(i)(2). Thus, the Act provides for no judicial review, even after the fact, of the AG's and DNI's certification that (a) a significant purpose of the surveillance is to obtain "foreign intelligence information" within the meaning of FISA; (b) that the surveillance is of people reasonably believed to be outside the United States; or (c) that the surveillance is not targeting a person believed to be in the United States.[4]

Third, the proposed FISA Amendments Act, like the Protect America Act, excludes from FISA's definition of "electronic surveillance" all of the communications intercepted under the authority granted by the Act. *See* Proposed Section 701.[5] As a result, the FISA Amendments Act excludes such communications from all of the protections of the FISA statute, including its provisions for civil and criminal liability for violations of FISA. There is no reason for this overbroad exclusion of such communications from the protections of FISA. As the proposed RESTORE Act shows, the goal of creating special procedures and rules to govern the interception of communications of individuals reasonably believed to be overseas can be easily accommodated without completely excluding such communications from all of the provisions of FISA.

Fourth, the proposed FISA Amendments Act authorizes the AG and DNI to issue a directive to a communications provider requiring the provider to comply, but does not require a court order directing the provider to comply. If the current dispute over immunity for telecommunications providers for their past participation in the Administration's arguably unlawful warrantless surveillance program teaches us anything, it is that communications providers should be entitled to the protection of a court order before they are obligated to participate. A court order would provide communications providers with the appropriate clarity and certainty that the directive to provide assistance is lawful and binding.

---

[3] In contrast, the RESTORE Act would authorize the FISA Court judge who approved the Administration's surveillance request to assess the Administration's compliance with these requirements. *See* RESTORE Act, Proposed Section 105B(e)(5).

[4] The RESTORE Act, in contrast, at least requires the FISA Court to assess the guidelines that will be used to ensure that the Administration in fact seeks an individualized warrant under FISA to conduct electronic surveillance of a person reasonably believed to be located in the United States. *See* RESTORE Act, Proposed Section 105B(b)(2)(D).

[5] Another provision of the FISA Amendments Act would redefine the communications intercepted under the Act as "electronic communications," but solely for purposes of Section 106 of FISA, which relates to the permissible use of the information obtained for law enforcement purposes. *See* Proposed Section 704.

Fifth, the proposed RESTORE Act, as part of the rigorous congressional oversight that it would establish, would require the Justice Department's Inspector General to conduct and submit to Congress an audit of all of the Administration's electronic surveillance programs since September 11, 2001, including the potentially unlawful surveillance activities that the Administration has fought aggressively to keep secret from the American public. Such an audit is an important step that should be taken to reassure the American public that the Administration's warrantless surveillance programs are, and will continue to be, subject to congressional oversight. The proposed FISA Amendments Act, however, does not include any such provision.

Sixth, the proposed FISA Amendments Act includes a sunset provision that terminates the authority granted under the Act in six years, on December 31, 2013. This is far too long. It is imperative that Congress have an opportunity, in the relatively near future, to reevaluate the necessity for the extraordinary authority granted by the Act, to examine how the Act has been implemented and what flaws it may contain, and to consider whether an approach more sensitive to protection of Americans' legitimate and constitutionally-protected privacy rights may be appropriate in light of the information obtained and experience gained under the Act. The proposed RESTORE Act pending in the House contains a two-year sunset provision, which the Association believes is an appropriate period to permit reconsideration in the next Administration. There is no reason to defer such reconsideration for six years, into the Administration after that.

Finally, the Association strongly opposes the provisions of the FISA Amendments Act that would retroactively grant immunity from liability to telecommunications companies that cooperated in the past with the Administration's unauthorized and probably unlawful warrantless surveillance program. There is no lawful basis for the Administration's demand for such absolute immunity, and there is no unfairness to the telecommunications companies in rejecting it. Nor should there be any reasonable concern that failing to provide immunity for this past conduct will jeopardize communications company cooperation in future surveillance programs.

The law in this area has been clear at all relevant times. Under 18 U.S.C. §2511(2)(a)(ii), telecommunications companies asked to participate in a government surveillance program are already entitled to immunity from suit as long as they receive either a court order directing them to provide assistance or obtain a certification by the Attorney General or his designee "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." Id. If the telecommunications companies obtained such a court order or certification, then they already have immunity under existing law, and there is no need for any additional grant of immunity. But if the telecommunications companies failed to obtain the required court order or certification, the grant of amnesty now would only reward their manifest failure to abide by the clear requirements of FISA's carefully tailored immunity provision. There is no excuse for this violation of law, even if it was done at the request of the Administration (but without the required certification of the Attorney General).

Contrary to the proponents of the FISA Amendments Act's immunity provision, immunity is not necessary to assure future cooperation with lawful surveillance demands. If the Administration's surveillance demand is lawful, the law already guarantees communications providers immunity from suit. The immunity demanded by the Administration thus provides protection only for unlawful surveillance demands. In these circumstances, the FISA Amendments Act's grant of immunity would encourage a culture of impunity for unlawful conduct, would undermine the rule of law, and would seriously erode incentives for future compliance with the law.

Sincerely,

Barry Kamins

cc: Hon. Harry Reid
Hon. Mitch McConnell

Senate Judiciary Committee

BARRY M. KAMINS
PRESIDENT
Phone: (212) 382-6700
Fax: (212) 768-8116
bkamins@nycbar.org

October 16, 2007

The Honorable Nancy Pelosi
Speaker of the House
U.S. House of Representatives
Washington, D.C. 20510

Dear Speaker Pelosi:

I write on behalf of the Association of the Bar of the City of New York ("the Association") to express the Association's views on two pending bills that would replace the Protect America Act hastily passed by Congress in August. Both the proposed RESTORE Act, H.R. 3773, introduced by Chairman John Conyers, Jr. of the Judiciary Committee and Chairman Silvestre Reyes of the Committee on Intelligence, and the proposed Foreign Intelligence Surveillance Modernization Act of 2007, H.R. 3782, introduced by Congressman Rush Holt, would restore to American citizens and residents at least some of the vital constitutionally-based protections against warrantless electronic surveillance previously mandated by the Foreign Intelligence Surveillance Act ("FISA").[1] Both bills would be a significant improvement over the inadequate protections against improper electronic surveillance temporarily adopted in the Protect America Act.

As discussed below, the Association believes that the Modernization Act is the better bill because it clarifies that FISA does not apply to "foreign-to-foreign" communications that happen to be routed through the United States – the principal rationale upon which the Administration has relied in seeking revisions of FISA – but is otherwise careful to protect the communications of U.S. persons against warrantless interception. Unlike the RESTORE Act, the Modernization Act requires an individualized FISA warrant to be obtained before the international communications of American citizens and residents could be intercepted, and would not authorize blanket advance approvals from the FISA Court for the surveillance of communications of people overseas that might include communications with persons inside the United States. The Administration has made no case for such blanket authorizations.

[1] This letter is a revised version of my letter on behalf of the Association dated October 15, 2007, which makes a minor factual correction and takes into account the amendments of the RESTORE Act agreed upon in committee mark-up last week, as reflected in the "Amendment in the Nature of a Substitute to H.R. 3773" prepared by the House Intelligence and Judiciary Committees, in the form available on October 15, 2007.

Nor has the Administration explained why the ordinary requirements of the FISA statute are not adequate to permit surveillance of the international communications of American citizens and residents, when necessary, and such blanket authority to engage in warrantless surveillance raises serious constitutional questions.

Nevertheless, the proposed RESTORE Act would go a long way towards correcting the deficiencies of the Protect America Act, and represents a compromise that the Association could accept. The RESTORE Act would give the Administration the power it has requested to intercept foreign-to-foreign communications without the obligation to obtain a warrant from the FISA Court, but it would do so in a way that is far more protective of the constitutional rights of American citizens and residents than the Protect America Act. The Protect America Act authorized the Attorney General and the Director of National Intelligence to intercept, without a FISA Court order, any communications "concerning" persons "reasonably believed" to be outside the United States, 50 U.S.C. § 1805b, as long as the Government was seeking foreign intelligence information. This authority was not limited to communications between persons outside the United States, and could be read to permit interception of communications entirely within the United States without warrants, a grant of authority that the Association believes to be plainly unconstitutional. Moreover, the Protect America Act granted the Attorney General and the Director of National Intelligence the power to authorize such interceptions on their own say-so, with no prior FISA Court review and with deferential after-the-fact judicial review, limited to the question whether the Government's determination that its procedures were reasonably designed to prevent improper interceptions of American citizens was "clearly erroneous," 50 U.S.C. 1805c. There is no basis for this extraordinary grant of virtually unreviewable authority to the Administration to carry out electronic surveillance potentially impacting U.S. persons. The Administration, to this day, has never made a cogent case that the procedures established under FISA impose unreasonable obstacles to electronic surveillance appropriate in the public interest.

While the Administration has provided no information to justify the RESTORE Act's provisions authorizing the Government to obtain blanket advance approvals from the FISA Court rather than individualized warrants – and the Association believes that such blanket authorizations fail to give adequate protection to legitimate privacy interests and raise serious constitutional questions to the extent they authorize warrantless interception of the international communications of American citizens and residents – the RESTORE Act would do a far better job than the Protect America Act of imposing appropriate limitations on the scope of the Administration's authority to conduct such electronic surveillance without an individualized court order.

First, the RESTORE Act would clarify that the surveillance authority it grants would only permit the interception of communications "of persons that are reasonably believed to be located outside the United States and not United States persons" (proposed Section 105B(a)), thus making clear that the Act does not permit warrantless electronic surveillance within the United States simply because it might "concern" people outside the United States.

Second, the RESTORE Act would return to the FISA Court a more meaningful role in reviewing applications to conduct electronic surveillance for purposes of gathering foreign intelligence. The Act would require the Administration to seek authority to engage in such foreign surveillance from the FISA Court in advance (apart from narrowly confined emergency situations), and require FISA Court approval of the procedures employed by the Administration in determining that targets are overseas; the information sought; the minimization procedures the Administration will follow; and the procedures the Administration will follow to ensure that individualized warrants are obtained under the FISA statute when surveillance of a person

inside the United States is required (proposed Section 105(b)(2)). These are all important checks on the Executive's exercise of the authority granted by the Act, and necessary to ensure that the authority granted is not abused.

Third, the RESTORE Act would require intensive oversight of the Administration's use of the power to obtain blanket authorization from the FISA Court for foreign electronic surveillance, oversight that is entirely missing under the Protect America Act. The RESTORE Act would require applications for blanket surveillance orders to be submitted promptly to Congress (proposed Section 105D(a)); regular audits of the use of this authority by the Justice Department's Inspector General (proposed Section 105D(b)); and regular reports to Congress from the Attorney General and Director of National Intelligence (proposed Section 105D(c), (d)) and 105D(d)).

The RESTORE Act also contains several other important provisions to protect the rights of U.S. citizens and residents. The Act would once more emphasize that the FISA statute furnishes the sole statutory authority for the Administration to engage in electronic surveillance for purposes of gathering foreign intelligence (Section 8 of the substitute bill), thus repudiating the Administration's baseless claim that the "Authorization for the Use of Military Force" adopted on September 18, 2001 provided supplemental statutory authority to engage in foreign intelligence gathering activities relating to terrorism.

The RESTORE Act would also require the Administration to make a full accounting to Congress of all its electronic surveillance activities since September 11, 2001 (Section 10 of the substitute bill), including potentially unlawful surveillance activities that the Administration has heretofore fought aggressively to keep secret from the American public and to avoid any judicial review.

Finally, the RESTORE Act would provide that the authority granted to the Administration to obtain blanket approval of warrantless foreign surveillance would expire in two years, on December 31, 2009 (Section 17(a) of the substitute bill). This limitation ensures that Congress will have another opportunity, in the relatively near future, to reevaluate the necessity for the extraordinary authority granted by the Act and to consider again an approach more sensitive to protection of Americans' legitimate and constitutionally-protected privacy rights in light of the information obtained and experience gained under the RESTORE Act.

In light of these positive aspects of the RESTORE Act, the Association would accept House approval of the RESTORE Act as a compromise measure. That said, however, the Association believes that the FISA Modernization Act proposed by Congressman Holt provides more complete protection to Americans' constitutional rights, and would be a preferable bill. Unlike the RESTORE Act, the proposed Modernization Act would exclude from the scope of the FISA statute <u>only</u> communications "transmitted exclusively between or among persons reasonably believed to be located outside the United States and not known to be United State persons" (proposed Section 302), and would not provide any authority for "blanket" FISA Court authorization of warrantless electronic surveillance. The Modernization Act would thus appropriately limit revision of the FISA statute to the Administration's oft-stated rationale, the need to exclude foreign-to-foreign communications which happen to get routed electronically through the United States. In so doing, however, the Modernization Act would also make clear that the usual requirements of the FISA statute – including the requirement of an individualized FISA warrant before the interception of electronic communications – apply to communications between a citizen or resident in the United States and an individual overseas.

The Association believes that Americans have a reasonable expectation of privacy in the telephone calls they make and the electronic messages they send to friends and colleagues

overseas, and that these legitimate privacy interests should be protected as a matter of sound policy to the greatest degree possible consistent with the legitimate demands of national security. Moreover, electronic surveillance of such communications without an individualized warrant raises serious constitutional questions.

The Administration has never made any showing that compliance with the standard procedures specified in the FISA statute to authorize the interception of such international communications would interfere with intelligence-gathering activities legitimately employed to keep the Nation safe from terrorism. The Administration has shown no reason why the Government could not satisfy the FISA warrant requirement in appropriate circumstances, and the FISA statute has long given the Government the authority to take emergency action when truly required, subject to obtaining FISA Court ratification of its actions within 72 hours. The proposed Modernization Act would indeed expand this authority, permitting the Government up to a week before it is required to obtain FISA Court authorization (proposed Section 201), and provides a much more acceptable balance between the Government's legitimate intelligence gathering needs and the privacy rights of American citizens and residents.

Before closing, I should address two other matters that are not currently part of either the RESTORE Act or the Modernization Act, but may well be brought to the floor of the House through proposed amendments. Obviously, in light of the analysis set out in this letter, the Association strongly opposes any effort to permanently authorize or extend the life of the Protect America Act. As stated above, the Protect America Act provides woefully inadequate protection for Americans' constitutional rights; it improperly vests the Administration with broad and largely unreviewable authority to engage in warrantless surveillance that threatens Americans' right to privacy, without any showing of real necessity; and it eliminates all effective judicial review of the Administration's foreign intelligence surveillance, as previously provided by the FISA Court.

Finally, the Association also strongly opposes any effort to give immunity from liability to telecommunications companies that have allegedly cooperated in the past with the Administration's unauthorized and probably unlawful warrantless surveillance program. There is simply no lawful basis for the Administration's demand for such absolute immunity. It would encourage a culture of impunity for unlawful conduct that is entirely unacceptable, undermine the rule of law, and seriously erode incentives for future compliance with the law. There is no unfairness in permitting lawsuits against the telecommunications companies to go forward, because these companies have always had a safety-valve to escape liability if asked to cooperate with a government surveillance program. Under 18 U.S.C. §2511(2)(a)(ii), the telecommunications companies were already entitled to immunity from suit as long as they received either a court order directing them to provide assistance or obtained a certification by the Attorney General or his designee "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." Id. Given the pre-existing availability of this carefully tailored immunity provision, the grant of amnesty now would reward only manifest failures to abide by the law. Any telecommunications company that failed to observe this express and unequivocal legal requirement, and failed to seek assurance that its conduct was legal over the years during which the surveillance allegedly occurred, has no legitimate cause for complaint, and should be held accountable for its unlawful conduct.

Sincerely,

Barry Kamins

cc: Hon. John A. Boehner

Hon. John Conyers, Jr.
Hon. Lamar S. Smith

Hon. Silvestre Reyes
Hon. Peter Hoekstra

Hon Rush Holt

NY Congressional Delegation
NJ Congressional Delegation