



NEW YORK  
CITY BAR

PATRICIA M. HYNES  
**PRESIDENT**  
Phone: (212) 382-6700  
Fax: (212) 768-8116  
phynes@nycbar.org

June 12, 2008

The Honorable Nancy Pelosi  
Speaker of the House  
235 Cannon House Office Building  
Washington, D.C. 20515

The Honorable John Boehner  
House Minority Leader  
1011 Longworth House Office Building  
Washington, D.C. 20515

Dear Speaker Pelosi and Minority Leader Boehner:

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 version of the FISA Amendments Act that is apparently being considered as a compromise to resolve the impasse between the differing versions of FISA bills that have been passed by the House and the Senate. The Association has previously written to express its support for the House bill, H.R. 3773, which was passed by the House last fall, even though that bill is itself a compromise that does not provide as much protection for privacy rights as we believe warranted. The Association has also previously expressed its opposition to the bill passed by the Senate in February, S. 2248, which we believe contains many of the same fundamental flaws as the Protect America Act hastily passed by Congress last August. As explained in detail below, the compromise bill now under consideration regrettably is no compromise at all. In most respects, it is substantially identical to the Senate bill, and, like that bill, provides utterly inadequate protection for the privacy rights of American citizens and residents and the confidentiality of their international communications.

The negotiations to reach agreement on a compromise bill have been conducted behind closed doors, and it is hard to know the exact shape of the compromise bill that may emerge. Nevertheless, from media reports, it now appears that a compromise based on the Senate bill, with certain amendments proposed by Senator Bond, is under serious consideration.

We urge the House to reject this proposed compromise and to insist on a final bill that comes much closer to H.R. 3773. We recognize that the Bond compromise includes several amendments to the Senate bill – taken largely from the House bill – which we view as positive steps. In particular, the compromise currently under discussion apparently includes a provision stating that the Act provides the exclusive means for the Government to lawfully conduct electronic surveillance for foreign intelligence gathering purposes, thus foreclosing the Administration’s claim of inherent constitutional authority to engage in such warrantless surveillance. The bill also makes provision for a thorough review of the Administration’s warrantless electronic surveillance programs since September 11, 2001, which the Administration has heretofore aggressively opposed. These are both important steps towards putting

the nation's constitutional house in order, after the abuses of recent years, and we urge that they be included in any final compromise bill.

Apart from these provisions, however, the proposed Bond compromise bill is really no compromise at all, and on the whole, the compromise bill is largely indistinguishable from the Senate bill. Neither of the positive steps detailed above relates to the fundamental question of what the ground rules should be under which the Administration will be permitted to engage in electronic surveillance in the future. On that crucial question, the proposed Bond compromise contains the same basic flaws as the Senate bill, and continues to provide inadequate protection for the privacy rights of American citizens and residents.

The proposed compromise bill provides inadequate privacy protections in numerous respects:

1. First, the compromise proposal, like the Senate bill, gives the Attorney General ("AG") and the Director of National Intelligence ("DNI") the authority to conduct warrantless surveillance on their own certification, without advance judicial review or approval. The compromise bill permits the AG and DNI, on their own authority, to initiate surveillance of persons believed to be outside the United States – including their communications with persons inside the United States. Rather than requiring any advance judicial approval – not even the kind of broad, programmatic warrant authorized by the House bill – the compromise bill merely requires the AG and DNI to prepare and file a certification with the FISA Court, certifying that the surveillance is targeted at someone reasonably believed to be outside the United States; that the surveillance is not intentionally acquiring communications where all of the participants are known to be in the United States; that there are reasonable targeting and minimization procedures in place which have been approved by (or will be submitted for approval to) the FISA Court; that these procedures are, in the judgment of the AG and DNI, consistent with the Fourth Amendment; and that "a significant purpose" of the surveillance is to obtain foreign intelligence information.

The bill requires this certification to be submitted to the FISA Court for approval, but the Administration may go forward with the surveillance as soon as the certification is submitted (and in emergency situations, even before it is submitted); may continue surveillance while FISA Court review is ongoing; and may continue surveillance even after an adverse FISA Court ruling for as long as the Government's appeal is pending. As a practical matter, this enables the Administration to engage in warrantless surveillance for an almost unlimited period of time without FISA Court approval, and makes a mockery of the requirement for FISA Court review. The significance of FISA Court review is further undermined by the inadequate standard of Court review permitted by the bill, as discussed below.

Moreover, wholly apart from the inadequate judicial review mandated by the bill, the opportunities for abuse permitted under the loose standards of the proposed bill are manifest. The bill permits the Administration to knowingly acquire the communications of people in the United States without judicial authorization, as long as at least one of the parties to the communication is reasonably believed to be outside the United States. The bill requires only that "a" significant purpose of the surveillance be to gather foreign intelligence information, and permits surveillance even if the Government has other significant or even predominant purposes. And, in requiring only that a purpose of the surveillance be to gather "foreign intelligence," the bill does not even limit the scope of the extraordinary authority it grants to addressing any terrorist threat – the only justification for its radical departure from traditional Fourth Amendment requirements – and could equally be employed to conduct warrantless surveillance of communications relating to our relations with friendly foreign governments.

2. The compromise bill does not provide for adequate judicial review by the FISA Court, and indeed deprives the FISA Court of any meaningful role in the Administration's electronic surveillance activities. Apart from the fact that the FISA Court's review comes long after the surveillance has been initiated (and is not necessarily effective to stop it), the scope of the judicial review authorized by the bill is inadequate. The bill authorizes the FISA Court to review the Administration's targeting procedures to assess whether they are reasonably designed to ensure that the surveillance is targeting persons outside the United States (and is not intentionally acquiring communications where all of the participants are in the United States). The bill also authorizes judicial review of the Administration's minimization procedures to assess whether they comply with the law. But the bill does not permit any other substantive judicial review of the certification submitted by the AG and DNI. On the contrary, the bill merely authorizes the FISA Court to determine whether the certification "contains all the required elements." As a result, the bill does not authorize any judicial review as to (1) whether the decision to target a particular individual or group is consistent with the targeting procedures in place; (2) whether the Administration's assertion that the participants are believed to be outside the United States is reasonable; (3) whether there really is a significant foreign intelligence gathering purpose; or (4) whether the surveillance itself (and not simply the Administration's targeting and minimization procedures) really does comport with the Fourth Amendment.

3. The bill excludes from FISA's definition of "electronic surveillance" all of the communications intercepted under the authority granted by the Act. As a result, the bill would exclude 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.

4. The bill would authorize the AG and DNI to issue a directive to a communications provider requiring the provider to comply, but does not require a court order; instead, it puts the burden on the communications provider to challenge the directive if it wants to obtain a binding judicial ruling as to its obligations. If the current dispute over immunity for telecommunications providers should teach us anything, it is that communications providers should be entitled to the protection of a court order before they are obligated to participate in the Administration's warrantless surveillance activities.

5. The bill in effect retroactively grants immunity to telecommunications companies that cooperated with the Administration's unauthorized – and probably unlawful – warrantless surveillance program. Although the bill purports to delegate this decision to the FISA Court, in fact the authority of the FISA Court is so circumscribed as to turn that Court into a rubber stamp for the Administration. The bill formally transfers jurisdiction of all cases challenging the providers' participation in the Administration program to the FISA Court, upon the certification of the Attorney General that the provider's actions were in response to a written request by the Administration which represented that the activity was "authorized by the President" and "determined to be lawful." But the bill does not give the FISA Court any power to review the substance of that certification, and merely provides that the case "shall be dismissed" as long as the Attorney General files a certification satisfying the bill's requirements. Since it is perfectly obvious that the bill has been drafted so as to make sure that the Attorney General will be able to provide such a certification – presumably, the Administration did provide a writing of some kind to the telecommunications providers stating that the request was authorized by the President and that it had been determined (by the Administration) to be lawful – the FISA Court's review turns out to be no review at all. This provision, like others in the bill, thus makes a mockery of the FISA Court's role, and is demeaning to that Court.

There is no lawful basis for the grant of such absolute immunity to the communications providers for their participation in the Administration's program. The law already provides that

telecommunications companies asked to participate in a government surveillance program are entitled to immunity as long as they receive either a court order directing them to provide assistance or a certification by the Attorney General that no warrant or court order is required by law. If the telecommunications companies participated in the Administration's warrantless surveillance program without obtaining either the required court order or certification, a grant of amnesty now would only reward their manifest failure to abide by the clear requirements of FISA's carefully tailored immunity provision.

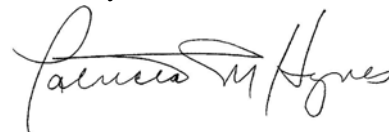
Finally, it should be noted that the Senate bill does not transfer jurisdiction of these cases to the FISA court, and requires the Attorney General to file such certifications in the district court in which the case is pending. In this respect, the proposed compromise is even worse than the Senate bill. There is no reason to authorize the transfer of these cases from a public forum to the secret FISA Court, which will result in removing from public scrutiny even the Administration's efforts to dismiss these cases.

6. The sunset provision of the bill – until December 31, 2013, or approximately five and one-half years – is far too long, and 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. There is no valid reason to postpone congressional reexamination of this authority beyond the administration of the new President to be elected this fall.

In contrast, the House bill would give the Administration the power it has requested to intercept foreign-to-foreign communications without the need for 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. The House bill would authorize the Administration to obtain blanket advance approvals from the FISA Court, rather than individualized warrants, but does a far better job of imposing appropriate limitations on the Administration's authority to conduct electronic surveillance without an individualized court order. The House bill 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 would return to the FISA Court a meaningful role in reviewing applications to conduct electronic surveillance for purposes of gathering foreign intelligence. Moreover, the House bill contains an appropriate sunset provision, until December 31, 2009, which would require reconsideration of the necessity for such extraordinary measures early in the Administration of the next President. And the House bill does not include the provisions of the compromise bill in effect granting telecommunications providers retroactive immunity for their participation in the Administration's warrantless surveillance activities.

For all of these reasons, the Association urges the House to decline to accept the compromise bill that is apparently being considered, and to insist on the provisions of its own bill in its continuing negotiations with the Senate.

Sincerely,



Patricia M. Hynes

cc: Hon. John Conyers, Jr.  
Hon. Silvestre Reyes  
Hon. Lamar S. Smith  
Hon. Peter Hoekstra  
New York Congressional Delegation