CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

March 12, 2008

Re: Vote "Yes" on H.R. 3773, the FISA Amendments Act

Dear Representative:

We are writing to urge you to support legislation to amend the Foreign Intelligence Surveillance Act that the House of Representatives will soon consider. The bill, an amendment in the nature of a substitute to H.R. 3773, is a responsible compromise between the House RESTORE Act and the Senate FISA legislation. This compromise includes most of the civil liberties protections in the RESTORE Act while also providing the intelligence agencies the flexibility they need to monitor the international communications of people believed to be abroad. The legislation would replace the Protect America Act ("PAA," Pub. L. No. 110-55), which became law in August 2007 and which expired a few weeks ago.

Like the RESTORE Act, the compromise bill permits authorization of surveillance programs targeting persons abroad who may be communicating with people in the United States. The compromise bill makes it clear that the government does not have to make an individualized showing of probable cause for targeting any person reasonably believed to be abroad, unless that person is a U.S. citizen or green card holder. It provides intelligence agencies great flexibility in adding new surveillance targets to existing authorizations. The compromise bill also makes it clear that no order is required for surveillance of foreign-to-foreign communications. The compromise bill includes no blanket immunity from civil liability for telecommunications carriers who assisted with illegal warrantless surveillance from October 2001 through January 17, 2007, but it does allow carriers to defend themselves against those lawsuits while protecting classified information.

Unlike the PAA, the compromise bill includes significant civil liberties protections that merit your support.

Prior Court Approval. Most importantly, the compromise bill requires court approval of surveillance procedures prior to the commencement of surveillance. Except in emergencies, the compromise bill bars the executive branch from commencing surveillance unless the Foreign Intelligence Surveillance Court ("FISA court") has approved of targeting and minimization procedures designed to protect Americans. The targeting procedures must be reasonably designed to ensure that communications to be acquired will be those of persons reasonably believed to be located outside the United States. The minimization procedures limit the circumstances in which a U.S. citizen or green card holder can be identified when information resulting from intelligence surveillance is disseminated. We are disappointed that under the compromise bill, the authorization for surveillance comes from the Director of National Intelligence ("DNI")

and the Attorney General ("AG"), and not from the FISA court, as would have been provided under the RESTORE Act. While we would have preferred the RESTORE Act approach, surveillance under both bills cannot commence unless the FISA court has first approved the procedures under which it would be conducted.

Court Compliance Assessment. The compromise bill explicitly authorizes the FISA court not only to assess the adequacy of surveillance procedures at the front end, but also to assess whether those procedures are being complied with on a going forward basis. It provides that the court shall assess compliance with the minimization procedures it has approved, and it acknowledges that nothing in the bill prohibits the FISA court from having inherent authority to assess compliance with those procedures and other procedures it has approved. While the extent of the court's inherent authority is unclear, we understand that the Administration has agreed that the court has inherent authority to assess compliance.

Prevention of Reverse Targeting. The compromise bill bars the targeting of a person reasonably believed to be outside the United States for the purpose of targeting a particular, known person reasonably believed to be in the United States. A number of provisions support this bar. They help ensure that surveillance targeted at persons abroad will not be used to circumvent individualized court order requirements that protect Americans from unwarranted surveillance. The bill requires the AG, in consultation with the DNI, to adopt guidelines to ensure compliance with the reverse targeting limitation. Those guidelines must contain criteria for determining whether a "significant purpose" of an acquisition is to acquire the communications of a specific, known U.S. citizen or lawful permanent resident reasonably believed to be in the United States. Those criteria must in turn reflect consideration of criteria listed in the bill that tend to show whether a person in the U.S. has become of significant intelligence interest. The guidelines must be submitted to Congress. AG/DNI certifications submitted to the FISA court in connection with authorized surveillance are reviewed by the FISA court for completeness, and must attest that guidelines meeting the reverse targeting limitation have been adopted. The Inspectors General and the AG/DNI both report to Congress on whether the reverse targeting guidelines are being followed.

FISA Exclusivity. The compromise bill takes a significant step toward the goal of clarifying that FISA is the exclusive means of conducting surveillance in the United States for foreign intelligence purposes. It does this by cutting off the argument advanced by the Administration that Congress may implicitly authorize warrantless surveillance when it authorizes the use of force following an attack on the United States, or when it passes other legislation. Under the bill, such authorization would need to be explicit.

Telecom Immunity. Unlike the Senate bill, the compromise bill wisely rejects proposals to grant blanket retroactive immunity to telecommunications carriers that assisted with illegal warrantless surveillance for more than five years following the attacks of September 11, 2001. Telecoms should be immune when they assist surveillance that meets the statutory requirements, and should face civil liability when they assist with

requests for assistance with unlawful surveillance. The compromise bill preserves this incentive system, which helps ensure that telecoms prevent unlawful surveillance. In lieu of retroactive immunity, the compromise bill frees telecoms to present in court information tending to show that they complied with the law, even though such information may be subject to the state secrets privilege. It signals that courts that such submissions must be protected from disclosure and should be handled in accordance with the relevant provision of FISA, Section 106(f).

The compromise bill also includes the following significant provisions:

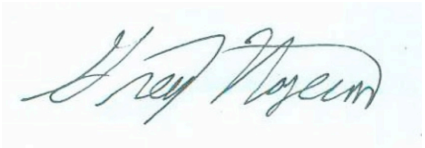
- A **December 31, 2009 sunset** to prompt Congress to reconsider the legislation in a timely manner, and to encourage Executive branch compliance with reporting duties imposed in the legislation and with congressional requests for information;
- An **Inspectors General audit** of post 9-11 warrantless surveillance that may represent the best chance of shedding light on this surveillance, to the extent consistent with national security concerns; and
- A requirement for **court orders based on probable cause** for surveillance of Americans and green card holders who are believed to be abroad, in lieu of the Attorney General certification of probable cause now required by executive order.

For all of these reasons, we encourage you to vote for the compromise bill when it is considered by the House of Representatives. It represents a responsible effort to preserve both liberty and security, and it is legislation the Administration would be wise to support.

For more information, please see our latest policy brief on FISA legislation (http://www.cdt.org/publications/policyposts/2008/3) or contact the Director of CDT's Project on Freedom, Security & Technology, Gregory T. Nojeim, at 202/637-9800 x113.

Sincerely,

Leslie Harris
President and CEO



Gregory T. Nojeim
Director, Project on Security & Technology