The New FISA Bill: A Bad Deal

The FISA deal announced on June 19 effectively grants retroactive immunity to companies that allegedly participated in the President's illegal wiretapping program, and it does not provide adequate protections for innocent Americans. Title I of the new bill, which includes a dramatic expansion of the Foreign Intelligence Surveillance Act, does not include the most significant safeguards approved by the Senate Judiciary Committee, and it does not include any of the amendments that Senator Feingold offered on the Senate floor earlier this year, each of which received 35 or more Democratic votes. These safeguards would have permitted the government to obtain the intelligence information it needs while also protecting the privacy of law-abiding Americans.

Background

The purpose of the bill is to address a problem that everyone agrees should be fixed – namely, making clear that the government does not have to get a warrant for foreign-to-foreign communications that happen to pass through the U.S. The new bill goes far beyond this narrow fix, however. It allows the government to listen in on international communications to and from law-abiding Americans in the U.S. who have no connections to terrorism, and the checks on this international dragnet authority are entirely inadequate.

Unjustified Grant of Retroactive Immunity

Under the new FISA bill, H.R. 6304, the immunity outcome is predetermined. A federal district court could review in secret the letters to companies to determine whether 'substantial evidence' indicates that they received written requests stating the activity was authorized by the President and determined to be lawful. But information declassified by the Senate Intelligence Committee already indicates that the companies got such written requests – meaning immunity is virtually guaranteed. The plaintiffs could participate in briefing to the court, but only to the extent it does not necessitate the disclosure of classified information, which will seriously impair their ability to participate in a meaningful way.

Lengthy Sunset

The bill sunsets in December 2012, a mere one year earlier than the Senate bill and a presidential election year.

Little Protection Against Reverse Targeting

The bill prohibits intentionally targeting a person outside the U.S. without an individualized court order if "the purpose" is really to target someone reasonably believed to be in the U.S., and it requires the executive branch to establish guidelines for implementing this requirement. But the guidelines are not subject to judicial review, and the bill does not include provisions approved by the Senate Judiciary Committee bill that would require the government to obtain a court order whenever a <u>significant</u> purpose of the surveillance is to acquire the communications of an American. This important "significant purpose" language had the support of 38 Senators when offered on the Senate floor, and was included in the House bill.

No Prohibition on Bulk Collection

The bill does not include a prohibition on bulk collection – the collection of all international communications into and out of the U.S. to a whole continent or even the entire world. Such collection would be constitutionally suspect and would go well beyond what the government has says it needs to protect the American people. This protection was in the Senate Judiciary Committee bill, and it garnered the support of 37 Senators on the Senate floor.

Loophole for Advance Judicial Approval of Court Orders

Under the bill, surveillance can begin after the FISA Court authorizes the program, or if the Attorney General and Director of National Intelligence certify that they don't have time to get a court order and that intelligence important to national security may be lost or not timely acquired. This broad 'exigency' exception could very well swallow the rule, and undermine any presumption of prior judicial approval.

No Limits on Use of Illegally Obtained Information

If the government goes forward with surveillance before obtaining court approval, and the court subsequently determines that the government's surveillance violated the law, the government can nonetheless keep and use any information it obtained. The compromise does not include a provision from the Senate Judiciary Committee bill that gives the FISA Court discretion to impose restrictions on the use of information about Americans acquired through procedures later determined to be illegal by the FISA court. This amendment had the support of 40 Senators on the Senate floor.

Few Protections for People in the United States

The bill does not include anything similar to the amendment offered by Senators Feingold, Webb and Tester (with 32 other Senators supporting) to provide additional checks and balances for Americans at home whose international communications are obtained because they are communicating with someone overseas, while also allowing the government to get the information it needs about terrorists and purely foreign communications.

Some Areas of Improvement

The bill contains some areas of improvement, but they do not address the serious privacy problems with the Senate bill.

- The bill contains strong language making clear that FISA and the criminal wiretap laws are the exclusive means by which electronic surveillance may be conducted.
- The bill contains an Inspector General review of the so-called "Terrorist Surveillance Program."
- The bill no longer redefines the key FISA term of "electronic surveillance."