

Center for National Security Studies

Protecting civil liberties and human rights

Director
Kate Martin

Deputy Director
Lisa Graves

June 25, 2008

Memorandum to Interested Persons From The Center for National Security Studies

Re: Title I of the FISA Amendments Act is a Major Setback for Americans' Privacy

We strongly oppose H.R. 6304, the FISA Amendments Act, and urge you to vote “No” on the bill. This legislation fails to restore judicial safeguards for Americans’ privacy and invites future abuses by failing to give the Foreign Intelligence Surveillance Court the necessary authority to protect law-abiding Americans from being spied on by their government. This memo addresses only the provisions authorizing surveillance of Americans; we also oppose the bill because it grants retroactive immunity to telecommunications carriers who cooperated with warrantless surveillance of Americans.

As noted by the Center for American Progress:

The bill is not without its positive features [including] a new requirement of probable cause for surveillance of Americans abroad. . . . Nevertheless, despite these welcome improvements, the bill fails at the most fundamental level to restore the independent judicial check on executive power that the Bush administration has done so much to undermine. Now, instead of determining whether probable cause exists for the issuance of a surveillance order, the FISA Court will be reduced to reviewing the adequacy of the surveillance procedures established by the Bush administration.

New Domestic Spying Legislation Fails to Restore Judicial Safeguards,” Mark Agrast, June 20, 2008, <http://www.americanprogress.org/issues/2008/06/unwarranted.html>.

1. The bill would authorize massive surveillance of Americans’ international communications. As more than 25 groups concluded: “The [Bond compromise] bill allows the government to intentionally acquire millions of Americans’ international communications with no individualized warrant or determination of probable cause, so long as one party to a phone call or e-mail is believed to be located abroad and the purpose is to gather foreign intelligence. “ (June 9, 2009 letter urging opposition to the FISA “compromise” proposed by Senator Bond from the ACLU, Center for American Progress Action Fund, Center for Democracy and Technology, Center for National Security Studies and Open Society Policy Center, among others.) While the proponents of the bill stress that the bill requires the “target” of the surveillance to be overseas, the purpose of the legislation is to authorize the acquisition of communications by Americans with persons overseas; purely foreign to foreign communications have always been outside the scope of FISA, even when acquired in the United States.

This bill would authorize much broader surveillance of Americans than the surveillance described by the President as the “Terrorist Surveillance Program,” where one end of the communications was overseas and at least one end was a suspected terrorist. In contrast, this bill imposes no requirement that the surveillance involve foreign terrorists and those suspected of conspiring with them. There is not even any requirement that the overseas “target” be a suspected “agent of a foreign power” or

“foreign power”, the categories that were permitted as targets under FISA. And there is no requirement that the purpose of such surveillance be to obtain information related to terrorism. To the contrary, the definition of foreign intelligence information is so broad as to sweep in virtually anything relevant to the national defense, security or foreign affairs.

This bill would authorize much broader surveillance of Americans’ international communications than was allowed under FISA. At a time when more Americans have more communications with friends, family and colleagues living, serving, or visiting abroad than ever before, Congress should be providing greater privacy protections, not fewer. Yet the standard which the government must meet under the bill is so low as to permit the vacuuming up of untold numbers of international phone calls and e-mails of American residents and businesses from the telecommunications infrastructure in the US. For the past 30 years, prior to the passage of the Protect America Act, FISA prohibited such surveillance here without an individualized court order. Absent a court order based on probable cause, FISA barred the acquisition in the United States of communications “to or from” persons in the U.S. regardless of whether a particular American was targeted or whether the target was someone overseas. Indeed, FISA was enacted to prevent electronic surveillance programs like Operation SHAMROCK, in which the NSA surreptitiously collected almost all international telegrams to or from Americans and analyzed them for foreign intelligence information.

In sum, the substantive standard which the government must meet in order to acquire Americans’ international communications is so low that it would authorize “vacuum cleaner” surveillance. This change in substantive standard alone eviscerates any judicial review.

2. The bill would eliminate, rather than restore, the meaningful judicial review required in FISA.

Instead of requiring court authorization of surveillance that intentionally and knowingly acquires the international communications of Americans in the U.S., this bill restricts judicial scrutiny to review of “targeting” and “minimization” procedures adopted by the government. While the proponents of the bill argue that such review is more than that provided in either the Protect America Act or the bill passed by the Senate (S. 2248), the review is wholly insufficient to protect Americans’ privacy rights. (Indeed, the bill does not even include key improvements to this scheme that were passed by the House or proposed as amendments in the Senate, which would have given some teeth to review of those procedures.)

The court review of the surveillance is limited to checking boxes. The court must review: the AG/DNI’s certification for completeness; the targeting procedures used to determine that the target is reasonably believed to be located abroad; and whether the minimization procedures meet statutory requirements.

Contrary to the assertions of some, *none* of the protections of FISA apply, unless the government “targets” an American by using her/her phone number or e-mail address to program its surveillance equipment. It is ironic that so long as the government does not identify a particular American, it would be free to seize millions of Americans’ communications. While we are pleased that the bill deleted the Senate “carve-out” to the definition of “electronic surveillance,” this did nothing to restore basic protections against acquisition of US person communications contained in FISA. Instead the bill eliminates longstanding safeguards, so long as a specific known U.S. person is not being “targeted”:

- No individualized judicial authorization of surveillance – only approval of program procedures.

- No determination of probable cause that any party to the seized communication is suspected of being a terrorist or spy.
- No requirement that the court be informed of the identity of the targets.
- No requirement that the Attorney General and the Director of National Intelligence “identify the specific facilities, places, premises or property at which the acquisition . . . will be directed or conducted.”
- No requirement that the court be informed of which telecommunications companies will be directed to assist in the surveillance.
- No requirement that the court be informed of the location of any physical searches that are conducted under this new acquisition authority.

While we believe that the Fourth Amendment mandates such requirements—and FISA surveillance has been upheld as constitutional because it required such showings—even those with a less generous view of the Constitution’s protections may not deny that this bill represents a sea change in statutory protections for Americans’ privacy.

Even if this bill did not offend the Constitution’s bar on “general warrants,” which it plainly does, the scope of surveillance offends the reasonableness requirement of the Fourth Amendment. It is not reasonable to allow the government to acquire and datamine millions of private communications of Americans in the indiscriminate search for foreign intelligence information.

3. The minimization requirements do not provide meaningful privacy protections.

The bill requires the court to determine that the minimization procedures adopted by the government meet FISA’s requirements for minimization. Those statutory requirements (50 U.S.C. 1801(h)) were enacted in 1978 to deal with the individualized surveillance authorized by FISA. It is hard to see how they will provide any protection or real limitation on the blanket surveillance being authorized in this bill. On the contrary, the minimization requirements essentially restate the broad foreign intelligence purpose requirement: Americans’ communications can be acquired, retained and disseminated “consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information” or where “necessary to understand foreign intelligence information or assess its importance.” 50 U.S.C. 1801(h).

Rather than providing for meaningful minimization, under this bill the NSA will be permitted to acquire millions of international communications by Americans, it will be allowed to keep them, datamine them and share them with other agencies. Minimization will not prevent the government from constructing a giant map of Americans’ social, political and employment associations and contacts that can be electronically enhanced with the billions of items of information on Americans now stored in government databases. Indeed, the bill authorizes collection of the information that will be used to construct that map.

Amendments to FISA may well be needed to ensure necessary intelligence-gathering and properly focused efforts to identify real threats. But this bill—which has never been subject to public hearing, markup or debate—sweeps far more broadly than the circumstances require or the Constitution permits. For all of these reasons, we strongly urge you to vote against this legislation.

For more information, please contact Center for National Security Studies, Lisa Graves or Kate Martin, lgraves@cns.org, kamartin@gwu.edu, 721-5650.