WASHINGTON
LEGISLATIVE OFFICE

June 25, 2008

Vote NO on H.R. 6304, the FISA Amendments Act – Oppose Warrantless Surveillance and Immunity for Telecommunications Companies

Dear Senator,

The American Civil Liberties Union strongly urges you to vote "NO" on H.R. 6304, the FISA Amendment Acts of 2008. This bill unconstitutionally and unnecessarily permits the government to vacuum up Americans' international communications, without a connection to al Qaeda, terrorism, or even to national security. While there is limited prior review by the Foreign Intelligence Surveillance Court, the protection afforded by that review is almost completely illusory. H.R. 6304 also grants retroactive immunity to companies that facilitated warrantless wiretapping over the last seven years. For these reasons, we ask you to stand with the Constitution and vote no on this overreaching legislation. Because this bill essentially eviscerates the Foreign Intelligence Surveillance Act and many of the Fourth Amendment protections it contained, we will be scoring this vote.

Our major concerns with this legislation include:

H.R. 6304 ensures the dismissal of all cases pending against the telecommunications companies that facilitated the warrantless wiretapping programs over the last 7 years. The test in the bill is not whether the government certifications were actually legal – only whether they were issued. Because issuance has been publicly documented, all the cases seeking to find out what these companies and the government did with our communications will be thrown out.[1] This immunity not only denies justice to those whom the government spied on in the last seven years, but undercuts the entire incentive structure in FISA and will encourage telecommunications company law breaking in the future. FISA has long contained provisions allowing Americans to seek civil redress in the courts, meaningful precisely in a situation such this where the government is complicit in the violation and criminal and other sanctions are highly unlikely.[2] If an entire industry is exempted from civil liability for violating long-standing privacy laws, it will send a message to all the companies in possession of our most sensitive information that compliance with statutory protections is optional, because congress will bail them out after the fact.

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] H.R. 6304, The Foreign Intelligence Surveillance Act Amendments Act of 2008, 110th Cong., §802. (hereinafter "H.R. 6304").
[2] 50 U.S.C. §1810.

H.R. 6304 permits the government to conduct mass, untargeted surveillance of all communications coming into and out of the United States, without any individualized review, and without any finding of wrongdoing. The official "targets" of the surveillance must be overseas, but this factor is of little comfort to the Americans who are on the other end of those communications. Americans do not lose their Fourth Amendment rights just because they participate in international communications. Americans who happen to be engaged in wholly innocent phone calls and email correspondence ought not to have their private communications captured, stored and used by their government without judicial oversight focused directly on the facts and circumstances surrounding the American-side of those communications.

H.R. 6304 legitimizes unconstitutional mass collection of Americans' communications,[3] first permitted by passage of the Protect America Act on August 5, 2007. These authorizations are not warrants at all because they are not directed at a particular individual. Instead, this bill authorizes entire programs of surveillance and requires only that they be directed outward and not intentionally target Americans or purely domestic communications. Called basket, bucket or blanket orders, the new court orders created by H.R. 6304 are most commonly known as "program" or "general" warrants and they violate the Fourth Amendment's requirement of particularity. The Fourth Amendment protects against unreasonable searches and seizures and government searches that are not specifically directed at those who are suspected of breaking the law. The Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Before the government may obtain a warrant for a search, it must identify with particularity the person or persons who are the target of the search. By authorizing the government to initiate surveillance programs in § 702, the proposed bill fails to meet this requirement. In direct contradiction, it states that certifications are "not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted."[4] Instead the new law authorizes general directives that need to state only that procedures exist to ensure that the "targets" of the programs are reasonably believed to be overseas.

Thus, H.R. 6304 permits the NSA to wiretap substantial numbers of unknown individuals in the United States, just as long as no United States person is the "target." The likely consequence is that U.S. persons communicating with those living, working or traveling abroad will have their communications swept up into the dragnet of communications obtained under non-individualized program warrants. From there, the NSA could pass along those conversations and the information could be misused even though the communications do contain no foreign intelligence information.

---

[3] H.R. 6304 §702(a).
[4] H.R. 6304 § 702(g)(4).

H.R. 6304 permits only minimal court oversight. The Foreign Intelligence Surveillance Court (FISC) only reviews general procedures for targeting and minimizing the use of information that is collected. The court may not know who, what, or where will actually be tapped, thereby undercutting any meaningful role for the court and violating the Fourth Amendment.

Under H.R. 6304 the FISC will be able to review three things: 1) the government's certification that it is not intentionally targeting Americans nor purely domestic calls; 2) targeting guidelines; and 3) minimization guidelines.[5] Thus, the FISC's role is nothing more than a generalized review of the proposed program. Such a review is a wholly inadequate role for the FISC and does little to protect the communications of Americans.

Proponents claim that the review of guidelines will ensure that the executive branch does not abuse this authority. In particular, they point to the provision in the bill that directs the Attorney General to promulgate guidelines to ensure that the new wiretapping programs will be targeted at "persons reasonably believed to be located outside the United States; and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[6] The Attorney General is also directed to adopt minimization procedures.[7]

While these two sets of guidelines will be reviewed by the FISC, it is not a substitute for individualized review, a judicial finding of apparent wrongdoing, and a directive to a specific entity for a specific communication collection. In fact, the legislative requirements for these guidelines in H.R. 6304 could not be more ambiguous. It is unclear what the government will actually submit to the FISC, and it is probable that the submission will contain insufficient detail for the court to make a meaningful decision about whether Americans' privacy is being protected.

Such a review is virtually meaningless because H.R. 6304 fails to set forth any kind of standard against which FISC judges could evaluate the procedures for lawfulness. Congress abdicated its responsibility to define the need for individualized orders and limit the use of U.S. information. Instead, Congress has left the executive branch in charge of negotiating our rights with a secret court. In the context in which matters will be presented, judges will likely defer to the government lawyers who are petitioning in secret for this authority.

Compounding this problem, the minimization procedures – the procedures designed to minimize the privacy impact on innocent Americans - have never been made public. No one, save a few Intelligence Committee members, knows whether minimization works or how it is actually implemented. Something so fundamental as giving government the authority to listen to our phone calls or read our emails should not be decided in secret by a handful of people. FISA, as amended, is largely silent as to statutory requirements providing guidance or limitations for those minimization procedures. The few provisions in FISA discussing minimization do not require that U.S. persons' information be destroyed – except in the case of wiretapping an embassy, a

[5] H.R. 6304 § 702 (i).
[6] H.R. 6304 §702(d).
[7] H.R. 6304 §702(e).

circumstance that does not apply to this program.[8] In the end, H.R. 6304 provides only a limited role for the FISC – to negotiate secret rules that do not even require that American information be destroyed, or ultimately prevent American information from being used or disseminated.

H.R. 6304 contains a general ban on reverse targeting – the practice of indirectly targeting an American by directing the surveillance at people overseas.[9] However, it lacks stronger language that was contained in prior House bills that included clear statutory directives about when the government should return to the FISA court and obtain an individualized order if it wants to continue listening to a US person's communications. For example, H.R. 3773, passed by the House in March required guidelines to force the government back to court when it became a "significant purpose" of the eavesdropping to actually pick up a specific U.S. person's communications.[10] These reverse targeting guidelines were required to address several factors, including whether a person was subject to repeated investigation or whether a person's information had been shared among agencies.[11]

Despite some claims to the contrary, the Attorney General is not required to promulgate reverse targeting guidelines by H.R. 6304. As discussed above, the targeting guidelines to be submitted to the court only need to include the procedures by which the government would determine 1) that targets are reasonably believed to be abroad, and 2) that the program won't intentionally collect purely domestic communications.[12] Instead of more comprehensive requirements, the government is left to determine if its surveillance of a foreigner has become a mere pretext to listen to a person located in American.

H.R.6304 contains an "exigent" circumstance loophole that thwarts the prior judicial review requirement. The bill permits the government to start a spying program and wait to go to court for up to 7 days every time "intelligence important to the national security of the US may be lost or not timely acquired."[13] By definition, court applications take time and will delay the collection of information. Depending on the interpretation, even a 30 minute delay could be seen by the most strident surveillance advocates as impeding 'timely' acquisition. The exception would swallow the rule. Proponents claim that this provision should frustrate prior court review only in rare circumstances – and we are heartened by such assurances. Nevertheless, this language does not track with the tried and true emergency provisions in FISA, implying that this new standard is not truly the "emergency situation."[14] We fear that future surveillance administrations will not constrain themselves to the assurances proffered by the proponents of this legislation. The administration appears to have had no qualms about violating the law outright in recent years and we fear it would have no problem exploiting the loose language of this provision to circumvent the FISC.

---

[8] 50 U.S.C. § 1801(h).
[9] H.R. 6304 § 702(b)(2).
[10] H.R. 3773, FISA Amendments Act of 2008, 110th Cong. § 702(f) (as passed by the House of Representatives on March 14,2008) (hereinafter H.R. 3773)
[11] Id.
[12] H.R. 6304 § 702(d).
[13] H.R. 6304 §702(c)(2).
[14] 50 U.S.C. § 1805(f).

The exigent circumstance loophole in H.R. 6304 is even more problematic because it lacks all of the back door minimization requirements in FISA's current emergency exception. Currently under FISA, if the government starts emergency surveillance, and then is denied the retroactive order by the FISC, the surveillance must stop and the information gathered cannot be used or distributed except to save life or limb.[15] Further, unless the government can show good cause to the FISC, the target must be notified of the illegal tap.[16] H.R. 6304 contains no such minimization and disclosure requirements when the court determines that exigent circumstances did not exist or the application was otherwise inadequate.

H.R. 6304 trivializes court review by authorizing the government to continue a surveillance program even after an application is denied by the court. The bill explicitly permits the government to continue entire surveillance programs even if the FISC finds that the application does not meet statutory or constitutional muster.[17] The government may even continue its spying for up to 60 days during the rehearing and appellate process, unless the court affirmatively intervenes.[18] Because these programs are vast dragnets, the two months it may take to obtain a final ruling to stop the surveillance may yield huge amounts of American information that can be used to the administration's desire – and to the detriment of the wholly innocent Americans' privacy rights.

Senators not on the Judiciary or Intelligence Committees are not guaranteed access to prospective reports from the Attorney General, Director of National Intelligence, and Inspector General. The two committees with jurisdiction over FISA will receive semi-annual reports from the Attorney General and the Director of National Intelligence about compliance with their own guidelines and annual Inspector General reports about the number of US persons whose information was disseminated in intelligence reports and the number of targets who were later determined to be in the U.S.[19] While this is a start, all 535 Members and Senators deserve access to not just to this information, but to much more. They deserve to know whether the information is being data-mined or otherwise used in a manner short of inclusion in an intelligence report; how Americans' information is handled; and other details relating to the effectiveness and intrusiveness of these new programs. So much of our concern with such surveillance programs relates to the absence of oversight and accountability. To bar even our own elected representatives from having access to this information suggests only that there is something improper about the programs. We believe not only that far more information should be provided about these programs, but also that this information should be accessible to all Senators and Members of Congress.

When the Protect America Act passed in August of last year, congressional leaders promised to fix that unconstitutional authority. We are dismayed that the resulting product writes many of those overreaching authorities into law for the next four years. We therefore ask you to stand up for the U. S. Constitution and vote 'NO' on H.R. 6304, the FISA Amendments bill, and take any

[15] 50 U.S.C. § 1805(f).
[16] 50 U.S.C. §1806(j).
[17] H.R. 6304 §§ 702(i)(3)(B), 702(i)(4)(B).
[18] H.R. 6304 §702(i)(4)(B).
[19] H.R. 6304 §702(l).

and all action necessary and possible to scuttle this unprecedented extension of governmental surveillance over Americans.

Sincerely,

Caroline Fredrickson
Director, Washington Legislative Office

Michelle Richardson
Legislative Counsel