

Congress Trying to Reconcile Competing Surveillance Bills

February 29, 2008

Tags: Array

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

The Senate and the House of Representatives have passed substantially different versions of legislation to amend the 1978 Foreign Intelligence Surveillance Act (FISA). House and Senate negotiators have been meeting in an effort to craft a compromise acceptable to both chambers. An agreement may be reached as soon as next week.

[1\) Congress Trying to Reconcile Competing Surveillance Bills](#)

[2\) Key Issue: Court Control over Surveillance Impacting Americans](#)

[3\) Cap on Damages Is Best Alternative to Telecom Immunity](#)

[4\) Expiration of PAA Should Have Limited Short-Term Impact](#)

1) Congress Trying to Reconcile Competing Surveillance Bills

The Senate and the House of Representatives have passed substantially different versions of legislation to amend the 1978 Foreign Intelligence Surveillance Act (FISA). House and Senate negotiators have been meeting in an effort to craft a compromise acceptable to both chambers. An agreement may be reached as soon as next week.

The new legislation would replace the Protect America Act (Pub. L. 110-55, "PAA"), hastily adopted last August. That Act permitted the government to eavesdrop without a court order on telephone and Internet communications between people in the United States and people abroad. The PAA did not require that the target be a suspected criminal or terrorist. Rather, the law required only that a significant goal of the surveillance was to collect broadly defined "foreign intelligence information" and that there were procedures in place making it reasonably likely that the surveillance targets were, in fact, abroad. Anchoring this new surveillance authority on the location of the target of surveillance failed to account for circumstances in which an American in the U.S., with privacy rights that must be protected, was on the other end of the line.

The Senate's new bill, the FISA Amendments Act (S. 2248, the "Senate bill") also provides only minimal protections to the rights of Americans affected by surveillance of communications to and from the U.S. In two important respects, the Senate bill is even worse than the PAA. While the PAA only lasted six months, the Senate bill would last six years. In addition, the Senate bill would undermine FISA's checks and balances by granting retroactive immunity to telecommunications carriers that assisted with the Administration's illegal warrantless surveillance activities for more than five years starting in October, 2001.

The House bill, the RESTORE Act (H.R. 3773), does a far better job of protecting civil liberties than does the Senate bill. The House bill gives substantially more supervisory authority to the Foreign Intelligence Surveillance Court (FISA Court), eschews telecom immunity, and has a short, two-year sunset period.

[A chart comparing the House and Senate bills](#) [1]

2) Key Issue: Court Control over Surveillance Impacting Americans

Telecom immunity has grabbed the media spotlight and overshadowed the more critical issue of judicial supervision. More recently, however, discussion of judicial supervision has been pushed as charges and counter-charges relating to expiration of the PAA have grabbed the most attention.

However, the role of FISA Court to approve and oversee surveillance impacting Americans is the most critical issue in the current debate. Unless the FISA Court retains a meaningful role, the privacy of Americans' international communications will be protected only at the whim of the executive branch. In virtually every regard, the authority of the FISA Court is clearer and stronger in the House bill than it is in the Senate bill, making it critically important that House negotiators insist on their provisions for judicial supervision.

Court Authorization of Surveillance

Prior judicial authorization of surveillance helps ensure that illegal surveillance never begins. Under the House bill, the FISA court authorizes surveillance of targets abroad who may be communicating with people in the United States. Under the Senate bill, the Attorney General and the DNI authorize such surveillance.

Under both bills, the FISA Court reviews targeting and minimization procedures designed to protect Americans, and the substantive requirements for those procedures are similar. The targeting procedures must be reasonably designed to ensure that the surveillance targets are located outside of the United States. The minimization procedures must give some limited protection to communications that are about or are with a U.S. person (a U.S. citizen or green card holder). Such communications may be shared with other agencies only if they contain foreign intelligence information, and the U.S. person's identity is concealed unless revealing it helps one understand the foreign intelligence information. (These are potentially very broad exceptions, but they are no change from prior law.)

A critical difference between the bills is that under the Senate bill, surveillance begins before the FISA Court has a chance to rule on the targeting and minimization procedures. Surveillance continues while the court decides whether to approve those procedures, and it continues if the FISA court disapproves them and the government opts to alter and re-submit the disapproved procedures to the FISA Court.

The Senate bill might actually bar the FISA Court from ordering cessation of surveillance that does not comply with the targeting and minimization procedures. Under the bill, the FISA Court can only order the government to choose between ceasing surveillance and altering the procedures that were disapproved. The government can repeatedly return to the court with slightly altered procedures while it continues the surveillance.

The House bill, as noted, puts judicial approval where it belongs - at the beginning of the process. In a huge concession to the government's arguments, the House bill does not require judicial approval of individual targets, even if they might communicate with someone in the U.S. Instead, the House bill creates a system of "program warrants" or "basket orders," under which the government can designate the individual targets on its own discretion.

The House bill also takes significant steps to cut off an argument used by the Administration to justify post 9-11 warrantless surveillance outside the requirements of FISA. The House bill's "exclusivity" provision indicates that a Congressional authorization of the use of military force should not be construed to authorize surveillance unless it does so explicitly. The Senate bill, in contrast, merely repeats current law. It therefore invites the argument that Congress might implicitly authorize warrantless surveillance in the future when it authorizes the use of military force.

Court Supervision and Termination of Surveillance

Court supervision of surveillance helps ensure that the targeting and minimization procedures approved by the FISA court are being followed. The degree of court supervision is limited and uncertain in the Senate bill. It provides that nothing in the bill should be construed to limit the FISA Court's inherent authority to enforce compliance with the orders it issues or with the procedures it approves. However, the scope of the FISA Court's inherent authority is unclear and subject to doubt. Moreover, there is little doubt that the Administration would argue that the FISA Court lacks inherent authority to oversee surveillance. The House bill, in contrast, specifically provides for FISA Court review of the implementation of the targeting and minimization procedures, and such review must occur at least quarterly. The House bill does not explicitly empower the FISA Court to order the government to alter its procedures following that review, or to order the termination of surveillance that does not comply with those procedures, and this omission should be corrected in the legislation that emerges from the current negotiations.

The House bill also includes a critically important provision that requires the government to cease surveillance authorized under the bill, and apply for a FISA Court order based on probable cause, when a "significant purpose" of surveillance targeting a person abroad is to collect the communications of a U.S. person in the U.S. This provides considerable protection for U.S. citizens and for lawful permanent residents who are in the U.S. It would preclude efforts to circumvent the Fourth Amendment's probable cause requirement by targeting people abroad for the underlying purpose of collecting the communications of a U.S. person in the U.S. The Senate bill, in contrast, has only a tautology: the NSA cannot target a person abroad for the purpose of targeting a person in the U.S.

CDT has testified to congressional committees about FISA on several occasions. [Our most recent testimony before the Senate Judiciary Committee was on September 25, 2007](#) [2]

[CDT's fact sheet on the House bill](#) [3]

[CDT's letter to the Senate opposing the Senate bill, and urging the Senate to adopt civil liberties amendments](#) [4]

3) Cap on Damages Is Best Alternative to Telecom Immunity

The Senate bill, unlike the House bill, provides blanket immunity from civil liability for communication service providers that assisted with illegal warrantless surveillance between October 2001 and January 17, 2007. The Administration has admitted that during this period, telecommunications carriers assisted the government with electronic surveillance conducted without a warrant. It argues that companies will not assist in the future with lawful surveillance unless also granted retrospective immunity for assisting with the illegal warrantless surveillance program. This argument carries little weight. The Senate and the House bills, and current law, all provide for prospective immunity for assistance with lawful surveillance, and give the government tools to compel that assistance.

Our nation's surveillance laws contemplate that carriers will cooperate with lawful surveillance requests and resist unlawful surveillance requests. The retroactive immunity sought by the Administration would undermine the structure and purpose of FISA by undermining the role that communications carriers play in effectively checking unlawful surveillance.

The logical compromise between the Senate position of full immunity and the House position of no immunity would be a cap on the damages that could be awarded for assistance with the unlawful surveillance program. The law provides for statutory damages of at least \$10,000 per person who was subjected to unlawful surveillance. When multiplied by the millions of customers of one of the large telecommunications carriers, damages could run into the billions of dollars and threaten to bankrupt the carrier. A cap on damages would protect them from ruinous damages, but preserve the role they play in being an impediment to unlawful surveillance.

4) Expiration of PAA Should Have Limited Short Run Impact

The PAA expired on February 16, 2008 amid recriminations, threats, and predictions of dire consequences if the law expired. In an effort to strong-arm the House into accepting the inferior Senate-passed bill, the President refused to accept an offer by Congress to extend the PAA for an additional 3 weeks. The Director of National Intelligence (DNI) took to the airwaves and the op-ed pages to warn that intelligence capabilities were being "degraded" and that "intelligence gaps" were opening because the PAA had expired and because retroactive immunity had not been granted to the telecoms.

In truth, not much will change in the short run. Surveillance orders issued under the PAA are good for one year, meaning that they that will not begin to expire until sometime in August at the earliest. These authorizations are broad and programmatic. They allow newly-discovered surveillance targets associated with known terrorist organizations to be added later, despite the expiration of the PAA. The PAA also enabled the DNI and the Attorney General to direct telecommunications carriers to assist with the authorized surveillance. Presumably, a court would interpret such directives to last as long as the surveillance authorization under which they were issued, although the PAA does not specifically say that, creating some level of uncertainty.

However, it does appear possible that a very limited class communications of surveillance targets might escape surveillance as a result of the expiration of the PAA. If a new terrorist organization emerges, its members could not be added as targets to surveillance authorized under the PAA. However, any time there was strong evidence that such a target was, in fact, a terrorist associated with such a group, the government could secure a surveillance order from the FISA Court to listen in on the new target. Moreover, the communications of such a target that are conveyed over the air (as opposed to over a wire passing through the U.S.) could in many circumstances be collected abroad, with no involvement of the FISA Court, and regardless of whether the PAA was reauthorized.

- [protect america act](#)

Copyright © 2008 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/policy/congress-trying-reconcile-competing-surveillance-bills>

Links:

- [1] <http://cdt.org/security/20080212FISACompare.pdf>
- [2] <http://www.cdt.org/security/20070925dempsey-testimony.pdf>
- [3] <http://www.cdt.org/security/20071017RESTOREActAnalysis.pdf>
- [4] http://www.cdt.org/security/20080205_FISA_ltr_.pdf