Bills Would Strengthen, Weaken Surveillance Standards

October 26, 2007
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:

Foreign intelligence - the process of collecting and analyzing information for the purpose of heading off attacks by foreign governments or terrorist organizations or otherwise protecting the national security or supporting diplomatic affairs - has long been recognized as essential to protect a country and its citizens. However, history has shown that, while intelligence is necessary, it can be abused. Consequently, the most intrusive types of intelligence gathering - electronic surveillance such as wiretapping, as well as physical searches - should be subject to judicial oversight when conducted in the United States or when targeting U.S. citizens at home or abroad.

(1) Intelligence Surveillance Requires Reasonable Checks and Balances

Foreign intelligence - the process of collecting and analyzing information for the purpose of heading off attacks by foreign governments or terrorist organizations or otherwise protecting the national security or supporting diplomatic affairs - has long been recognized as essential to protect a country and its citizens. However, history has shown that, while intelligence is necessary, it can be abused. Consequently, the most intrusive types of intelligence gathering - electronic surveillance such as wiretapping, as well as physical searches - should be subject to judicial oversight when conducted in the United States or when targeting U.S. citizens at home or abroad.

In 1978, to establish reasonable checks and balances on electronic surveillance for national security purposes, Congress enacted the Foreign Intelligence Surveillance Act (FISA). With limited exceptions, FISA requires the government, before conducting a wiretap or a physical search, to obtain a court order based on a finding of probable cause to believe that the person being targeted is a spy or a terrorist or other "agent of a foreign power." A special Foreign Intelligence Surveillance Court issues these orders. In 2006, it issued 2176 orders, the largest number in its 30-year history. Notably, while the court turned down only one government application, it made substantive modifications to the government's proposed order in 73 cases. In five other cases, the government withdrew its application before the court could act, presumably because the court had signaled a concern.

FISA has been updated with dozens of amendments since 1978, often to expand government power or weaken the checks and balances it provides. In the PATRIOT Act of 2001, Congress amended FISA to, among other things, permit the government to use the Act even when its primary purpose is not to collect foreign intelligence information. The PATRIOT Act also weakened FISA standards for government access to records that businesses hold about their customers.

Over the years, FISA was held to be constitutional and it worked fairly well: it afforded intelligence agency employees a degree of clarity and certainty in carrying out their duties, the court orders gave communications service providers assurance that their cooperation with government surveillance was lawful, and use of intercepted communications was permitted in criminal cases under clear rules.

A wealth of information about FISA is available, including the annual statistical reports of the FISA court. [1]

(2) In August, Congress Blessed Warrantless Surveillance

In December 2005, the New York Times revealed that the Administration had been intercepting communications to and from people in the US without a court order. The Administration essentially admitted that it was acting in violation of FISA, but argued that the President was not bound by the law.

Rather than working to develop a reasonable set of checks and balances suited to today's technology and threats, the Administration proposed a wholesale rewrite of FISA to ratify its activity and permit surveillance inside the United States without a court order.

The Administration initially argued that changes were needed to make it clear that a court order was not necessary to intercept communications between two terrorism suspects overseas. (As a result of massive investment in recent years in fiber optic cables to and from the United States, a large percentage of the world's communications, including many foreign-to-foreign communications, pass through the US and are thus available here to our intelligence agencies.) CDT and other civil liberties advocates agreed that FISA was not intended to cover foreign-to-foreign communications and suggested a narrow amendment to make that clear.

However, in a classic "bait-and-switch," the Administration drafted sweeping legislation to do much more than exempt foreign-to-foreign communications from FISA. Instead, it proposed exempting from any court supervision interception of essentially international communications, even calls to and from the US, even when an American in the US was a party to the communication.

This past August, amid dire warnings from the Administration that the terrorist threat had increased and that the intelligence agencies had lost their ability to function effectively, Congress passed the Protect America Act, substantially eroding FISA's checks and balances and essentially giving the Administration a blank check in intercepting any form of communication into and out of the US.

CDT's extensive resources on the Administration's warrantless surveillance activities and the Protect America Act [2]

(3) The Protect America Act Weakens FISA

The Protect America Act (PAA) adopted in August 2007 permits the government to eavesdrop on telephone and Internet communications between people in the United States and people abroad without a court order. Under this sweeping legislation, e-mail messages and telephone calls that an American has with a targeted person abroad can be acquired by the National Security Agency, stored, and shared with other governmental agencies. The target need not be a suspected criminal or a suspected agent of a foreign terrorist organization or government. The only criteria for the surveillance are that the "targeted" person is abroad and that a significant purpose of the surveillance is to collect foreign intelligence information.

The PAA has the barest fig leaf of judicial review, but it comes too late, covers too little, and is too weak.

- Too late: Under the PAA, months after the surveillance begins, the government must submit

to the FISA court a certification that it has put in place reasonable procedures to direct its surveillance against people reasonably believed to be abroad.
- Too weak: The FISA court can only assess whether the government's determination that its procedures are reasonable is "clearly erroneous."
- Too little: The court never reviews the minimization procedures that are supposed to limit dissemination to other agencies of information about US citizens, nor does it review how the government is implementing the surveillance. For example, the court has no power to order the Administration to obtain individual approval for surveillance that intrudes on a reasonable expectation of privacy of an American.

CDT has testified to Congressional committees about FISA on several occasions. Our most recent testimony, focusing on the PAA:
CDT Testimony, House Intelligence Committee [3] [pdf], September 18
CDT Testimony, Senate Judiciary Committee [4] [pdf], September 25

(4) House Legislation Would Restore Some Checks and Balances

Because it was acting under such pressure, and because it still had not received full information about the Administration's past violations of FISA, Congress put a "sunset" on the PAA: The Act expires on February 1, 2008. Congress is now considering alternatives that would provide greater judicial control while still giving the intelligence agencies the ability to select targets abroad with speed and agility.

In an ideal world, any time the government intercepted the communications of a person protected by the Constitution, it would be required to have a court order. However, when intelligence agencies are targeting people abroad, they have no way of knowing in advance, and often can't tell even at the time of interception, whether the targeted person is communicating with someone in the US. The challenge is how to create checks and balances to ensure that surveillance targeted at persons overseas does not unduly infringe on the privacy of people in the US.

To address this problem, two committees in the House of Representative have developed the concept of a "basket order," which they have recommended in legislation called the RESTORE Act.

The RESTORE Act requires the government to submit to the FISA court for review both the procedures for ensuring that the persons targeted are reasonably likely to be overseas and the procedures for handling any communications of Americans that are intercepted in the course of targeting those persons abroad. If the court finds the government's procedures to be reasonably likely to be effective, it issues an order authorizing surveillance of targets overseas chosen by the intelligence agencies.

Equally important, RESTORE Act also requires periodic reports to the FISA court, so it can supervise the implementation of the basket order. If, based on this review, the court finds that a particular surveillance targeting a person abroad has begun to focus on communications with an American, so that a "significant purpose" of the surveillance has become surveillance of the American, then the government to continue that surveillance must obtain a full, individualized court order based on probable cause.

The RESTORE Act is an improvement over the PAA, which has no prior court review at all and no judicial supervision to determine whether the government is complying with the targeting and minimization guidelines.

The RESTORE Act includes other important oversight mechanisms. It requires the Inspector General of the Department of Justice to conduct an important audit of the surveillance. The IG's reports would be submitted to the congressional intelligence and judiciary committees and to the FISA court.

The RESTORE Act would sunset on December 31, 2009, allowing Congress to revisit the legislation

and correct abuses, informed by the IG audit and other reports to Congress mandated under the bill.

The RESTORE Act also cleans up ambiguous language in the PAA that could have been interpreted to allow warrantless access to purely domestic communications between people in the U.S. that merely "concern" people believed to be abroad.

Under the RESTORE Act, communications service providers would be protected from liability for assisting with surveillance covered by basket orders, but, contrary to the wishes of the Administration, the bill would not grant immunity to those who violated FISA in the past.

CDT supports the RESTORE Act, but it believes that the bill could be improved, as the legislative process moves forward, by making it clear that the FISA court should cut off surveillance authorized under the basket court orders that infringes on the rights of any person in the US.

House Judiciary Committee report on the RESTORE Act [5]
House Intelligence Committee report on the RESTORE Act [6].

(5) So Far, the Senate Bill Leaves Too Much Discretion with the Executive Branch

Last week, the Senate Intelligence Committee recommended its own version of legislation to replace the expiring PAA. While the Senate bill, known as the FISA Amendments Act, takes some steps to increase the role of the FISA court, it is inferior to the RESTORE Act from a civil liberties perspective.

Like the PAA and unlike the RESTORE Act, the FISA Amendments Act gives to the Executive Branch the power to authorize surveillance - a power traditionally assigned to judges. Under the Senate bill, the court reviews both the minimization and targeting procedures, but, as under the PAA, the review takes place after surveillance has begun. Under the FISA Amendments Act, surveillance begins when the Attorney General and the Director of National Intelligence Authorize it, and it continues for as long as it takes the court to render a decision, it can continue for 30 days after an adverse decision by the court while the government moves to amend the guidelines, and it may continue while the government appeals any adverse ruling.

Under the Senate bill, rather than receiving a court order, communications carriers receive a directive from the Attorney General and the Director of National Intelligence compelling them to cooperate with the government's demands for assistance. A court order is far better, for it gives the carriers certainty when their assistance is sought. (The debate now over the Administration's past warrantless surveillance activity centers on whether carriers were justified in relying upon a claim of legality from the Attorney General. A court order means carriers don't have to guess. Under the RESTORE Act, they get a court order.)

Also, the Senate bill does not have an adequate procedure for the court to decide when a particular surveillance activity is affecting the rights of an American so much that it requires an individualized order. As we explained above, the House bill has a â€œsignificant purposeâ€? test - if a significant purpose of a particular surveillance becomes the collection and sharing of the communications of a US citizen, then an individualized warrant is necessary under the House bill. The Senate bill leaves it entirely to the Executive Branch to decide when things have gone so far that an individualized warrant is necessary.

Under the Senate bill, the court does not have clear authority to oversee implementation of the targeting and minimization procedures after they have been approved. The House's RESTORE Act requires the FISA court to assess compliance with the targeting and minimization procedures and guidelines. Under the Senate bill, at best the government must resubmit the procedures for review once a year, although it may be the case that once the procedures have been approved, the government can continue to use them indefinitely.

The Senate bill, like the PAA, is based on the very confusing approach of stating that certain

electronic surveillance is not "electronic surveillance" for purposes of FISA. Because so much of FISA turns on the definition of "electronic surveillance," this creates unnecessary confusion and ambiguity. The FISA Amendments Act then goes on to state that one part of FISA -- the provisions at 50 U.S.C. Section 1806 about use of information gleaned from electronic surveillance - DOES apply to surveillance that the bill has defined as NOT being "electronic surveillance." This cherry picking of particular sections of FISA to apply or not apply is likely to have unintended or unappreciated consequences. It seems, for example, that FISA's criminal penalties and civil liability for unlawful surveillance would not apply to surveillance authorized by the Senate bill, so government officials and service providers could violate even the generous rules of the Senate bill with impunity.

Any legislation that Congress enacts to replace the Protect America Act should address the question of exclusivity - the principle that the laws passed by Congress are the exclusive means for conducting electronic surveillance in the United States. The RESTORE Act strengthens FISA's exclusivity provisions and precludes any implicit statutory authorizations of surveillance. It is also intended to preclude surveillance based merely on the President's claim of inherent power, but this preclusion should be made more airtight. The FISA Amendments Act, in contrast, merely repeats current law, thus allowing a repeat of the uncertainty that has overshadowed foreign intelligence surveillance for the past six years.

The FISA Amendments Act as approved by the Senate Intelligence Committee would sunset on December 31, 2013 - six years from now. This seems too long to wait to revisit the Act to correct any abuses of the authority it grants or any unintended consequences of such complex and ambiguous legislation.

In at least two respects, the FISA Amendments Act is superior to the RESTORE Act. First, it requires an individualized FISA court order based on probable cause for acquiring the communications of any U.S. citizen or resident who is abroad. Since 1978, when FISA was adopted, no such court order has been required. Instead, the probable cause determination was left to the Attorney General. Requiring a particularized court order for surveillance in the United States that targets a U.S. person abroad is a small but positive development.

In addition, the FISA Amendments Act explicitly requires the FISA court to assess whether targeting and minimization procedures to be used in connection with surveillance targeting people abroad are consistent with the Fourth Amendment to the U.S. Constitution. While the court could make this assessment anyway, explicit statutory language calling for the court to disapprove surveillance procedures that are inconsistent with the Fourth Amendment is a welcome addition. While these two provisions are important, other problems with the FISA Amendments Act identified above make it a less favorable bill from a civil liberties perspective, and therefore CDT opposes the FISA Amendments Act. The best approach would be for Congress to pass the RESTORE Act, with these two provisions inserted in it.

The Senate bill [7] is available at the Intelligence Committee site.

(6) Retroactive Service Provider Immunity Would Undermine the Rule of Law and Create Ongoing Uncertainty

The Senate bill, unlike the House bill, provides blanket immunity from civil liability for communications service providers that assisted with illegal warrantless surveillance between September 11, 2001 and January 17, 2007. The Administration has admitted that during this telecommunications carriers assisted the government with electronic surveillance conducted without a warrant.

Telecommunications carriers have a dual responsibility under our nation's surveillance laws: to assist government surveillance and to protect the privacy of their customers. Without the carriers' cooperation with lawful surveillance requests, it would be much more difficult for the government to listen in when terrorists and criminals communicate. At the same time, however, without the carriers' resistance to unlawful surveillance requests, the privacy of innocent Americans'

communications would be threatened by zealous officials acting on their own perception, rather than the law's definition, of what surveillance is permitted and prohibited.

The retroactive immunity contemplated by the FISA Amendments Act would undermine the structure and purpose of FISA by undermining the role communications carriers play in effectively checking unlawful surveillance. Moreover, it would place service providers in an impossible position in the next crisis: if the government approached them with a request for surveillance that did not meet the statutory requirements, they would be uncertain as to whether they should cooperate in the hope that they would later get immunity.

The question of immunity has become tied up with the question of Congress' access to information about the Administration's past violations of FISA. The Senate Intelligence Committee included immunity in its bill after it received documents it had been seeking from the Administration. While it would be inappropriate for Congress to consider immunity legislation before the Administration explains what role communications carriers were asked to play in warrantless surveillance after the September 11 attacks, getting the documents does not justify full immunity.

Instead, CDT has recommended that Congress institute a cap on damages. A cap on damages would protect telecommunications carriers from ruinous damages, but it would preserve the role of the telecommunications carriers in being an impediment to unlawful surveillance.

-
- protect america act

Source URL: https://cdt.org/policy/bills-would-strengthen-weaken-surveillance-standards

Links:
[1] http://www.fas.org/irp/agency/doj/fisa/
[2] http://www.cdt.org/security/nsa/briefingbook.php
[3] http://www.cdt.org/security/20070918dempsey-testimony.pdf
[4] http://www.cdt.org/security/20070925dempsey-testimony.pdf
[5] http://www.rules.house.gov/110/text/110_hr3773rpt_judiciary.pdf
[6] http://www.rules.house.gov/110/text/110_hr3773rpt_intel.pdf
[7] http://intelligence.senate.gov/071019/fisa.pdf