



House approves another five years of warrantless wiretapping

Reauthorization of the FISA Amendments Act must still be passed by the Senate.

By: Timothy B. Lee

Sept 12 2012

The House of Representatives easily passed legislation on Wednesday to re-authorize the FISA Amendments Act, the 2008 law that allows the federal government to intercept the international communications of Americans with minimal judicial oversight. The vote was 301 to 118.

"I think that the government needs to comply with the Fourth Amendment to the Constitution all the time," said Rep. Zoe Lofgren (D-CA) in a floor speech opposing the bill. "We can be safe while still complying with the Constitution of the United States."

But House Judiciary Committee Chairman Lamar Smith, (R-TX) disagreed. "Foreign terrorists continue to search for new ways to attack America," he said before the vote. "Foreign nations continue to spy on America, to plot cyber attacks, and attempt to steal sensitive information from our military and private-sector industries."

But not all Republicans supported the legislation. One opponent was Rep. Tom McClintock (R-CA). "We're told, don't worry, the law requires that any irrelevant information collected in this manner be disregarded," McClintock said. "But here's the problem: the enforcement of this provision is itself shrouded in secrecy, making the potential for abuse substantial and any remedy unlikely."

The American Civil Liberties Union also blasted the legislation.

"Yet again, the House has rubberstamped a law so broad and vague that, despite its passage four years ago, we still have little idea how the government is using it," said Michelle Richardson, ACLU legislative counsel. "It is at the very heart of the Fourth Amendment that Americans and their communications are fiercely protected from government intrusion."

The return of general warrants

The FAA was originally enacted in the heat of the 2008 campaign season. During the primary, then-Sen. Barack Obama (D-IL) declared his opposition to a provision providing retroactive immunity to telecommunications companies that illegally participated in surveillance programs, vowing to filibuster the legislation if it came to the Senate floor. But once he secured the Democratic nomination for president, he switched sides and voted in favor of the bill.

The immunity provision received the most attention in 2008, but as we reported at the time, it wasn't the most troubling part of the bill:

The legislation establishes a new procedure whereby the Attorney General and the Director of National Intelligence can sign off on "authorizations" of surveillance programs "targeting people reasonably believed to be located outside the United States." The government is required to submit a "certification" to the FISA court describing the surveillance plan and the "minimization" procedures that will be used to avoid intercepting too many communications of American citizens. However, the government is not required to "identify the specific facilities, places, premises, or property" at which the eavesdropping will occur. The specific eavesdropping targets will be at the NSA's discretion and unreviewed by a judge.

Crucially, there appears to be no limit to the breadth of "authorizations" the government might issue. So, for example, a single "authorization" might cover the interception of all international traffic passing through AT&T's San Francisco facility, with complex software algorithms deciding which communications are retained for the examination of human analysts. Without a list of specific targets, and without a background in computer programming, a judge is unlikely to be able to evaluate whether such software is properly "targeted" at foreigners.

In a recent blog post, Julian Sanchez, a Cato Institute analyst and former Ars contributor, noted that this kind of broad surveillance power bears an eerie similarity to the "general warrants" that inspired the founding fathers to adopt the Fourth Amendment in the first place. During the colonial era, agents of the crown could obtain legal orders allowing them to enter any residence in search of criminals. These powers were sometimes used for fishing expeditions designed to smoke out "seditious" writers who criticized the government anonymously. To prevent this kind of abuse, the authors of the Fourth Amendment required that search warrants specifically describe "the place to be searched, and the persons or things to be seized."

Today, Sanchez writes, that logic is being stood on its head:

Modern defenders of the FISA Amendments Act argue that sweeping NSA surveillance of our digital "papers" is constitutionally unproblematic precisely because it does not "target" the Americans whose papers are searched: The groups or individuals who are the "targets" of programmatic NSA communications interception must be foreign. One wonders what the Founders would have made of this strange "defense": When the king's messengers burst into printer Dryden Leach's home in the dead of night to ransack his personal papers—acting on a secondhand report that John Wilkes had recently been seen in his shop—the fact that Wilkes and not Leach was the ultimate "target" of the search hardly excused it in the eyes of liberty-minded observers on either side of the Atlantic. What was so egregious was precisely that the messengers enjoyed "a discretionary power... to search wherever their suspicions may chance to fall," and not merely a power limited to the person and property of their specific "target."

While the FAA passed easily in the House, the fight is far from over. The bill must still be approved by the Senate, where Sen. Ron Wyden (D-OR) has placed a hold on the bill. Wyden has been pressing for more than a year to get basic information about the surveillance programs authorized by the FAA. Incredibly, the National Security Agency has claimed that it can't even give a ballpark figure for the number of Americans who have been subject to surveillance, because such a disclosure—not the spying itself—would violate the targets' privacy.

A legal challenge to the FAA has been working its way through the courts since it was originally approved in 2008. The government has argued that the plaintiffs, a group that includes journalists and civil rights groups, lack standing to sue because they cannot prove that they have personally been the target of surveillance under the law. The Supreme Court is due to hear arguments on that question on October 29.