WebMemo
Published by The Heritage Foundation
No. 2645
October 8, 2009

Freezing Telecom Immunity Would Chill Counterterrorism Efforts

Jena Baker McNeill

On September 17, Senator Russ Feingold (D–WI), along with several other Senators, introduced the Judicious Use of Surveillance Tools in Counterterrorism Efforts Act of 2009, which would remove immunity for telecommunications providers that have given federal law enforcement access to their systems under the National Security Agency's electronic surveillance program.

Stripping away immunity for telecommunications providers would roll back a key counterterrorism tool that helps law enforcement stop terrorism at its earliest stages. It would also decrease telecom providers' willingness to participate in national security investigations. The act constitutes an abandonment of the private sector, a vital partner in the war on terrorism.

Surveillance with Judicial Oversight. Enacted in 2001, the Patriot Act provides for electronic surveillance of individuals within the United States, with certain limitations. The act's provisions, such as the roving wiretap, allow authorities to track terrorists across different communication mediums, stopping terrorists from evading authorities by simply ditching one cell phone or e-mail account for another.

While this type of surveillance is commonly referred to as "warrantless wiretapping," it is far from warrantless. In fact, the Foreign Intelligence Surveillance Act (FISA) application required for such surveillance is significantly more burdensome than a common warrant. Coupled with significant legal authority and judicial oversight, the electronic surveillance program is ideal for dismantling terrorist networks.

One of the fundamental requirements of a successful surveillance program, however, is cooperation from the private sector. The reality is that government entities need telecom operators and other elements of the private sector to provide access to communications networks, conduct electronic surveillance, and provide information and technological expertise.

Legal Conundrum. Without proper immunity, cooperating with the government can be a risky proposition for the private sector. While the surveillance activities performed are entirely legal, stripping immunity would make way for dozens of lawsuits against telecommunications operators that assist the government with surveillance programs.

The nature of a surveillance program, however, makes it nearly impossible to defend against these charges because proving the legality would force the operators to divulge sensitive information, including methods of surveillance—information that would prove quite useful to terrorists looking to avoid detection. Also, because of the national security consequences associated with this sensitive

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/wm2645.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

information, the government is forced to raise a "state secrets" privilege when this information might possibly be divulged in a court of law. Consequently, telecom operators are facing a huge conundrum: They cannot prove their case without demonstrating that their methods are legal. Yet because of the sensitivity of the information involved, they are prohibited from disclosure.

Congress, however, gave the telecom providers retroactive immunity against suit in the FISA Amendments Act of 2008. This immunity is absolutely necessary to stop telecom operators from being the innocent victims of their own goodwill. Without this immunity, surveillance programs that are protecting Americans every day will be at risk.

One Step Forward, Not Back. Repealing telecom immunity would be a step backward for U.S. counterterrorism. Allowing telecom providers to be sued will send a message to the private sector that the government does not value their role in homeland security. But most importantly, the government simply cannot conduct these investigations alone: It needs the private sector. Congress should reject any legislation that would repeal this immunity. Specifically, Congress should:

- *Keep telecom immunity.* Congress should maintain immunity and look for additional ways to engage the private sector.
- *Reauthorize key provisions of the Patriot Act.* Congress should immediately reauthorize key provisions of the Patriot Act before the provisions expire on December 31. It should also resist measures that would dilute the act's integrity or erode key provisions that make the act successful. Doing so will ensure that America continues to have the right kind of counterterrorism tools at its disposal.
- *Promote the SAFETY Act.* An additional way to engage the private sector in counterterrorism is by promoting the use of the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. The SAFETY Act offers liability protection to companies if their technology is deployed in the event of an act of terrorism. The Department of Homeland Security should continue to look for better ways to inform companies about these protections and encourage their full participation. Bringing the private sector under this protection will facilitate the development and deployment of new and better technologies that will keep Americans safer.

Protecting America requires a strong private–public partnership. Consequently, private-sector immunity remains a key element of the electronic surveillance program. If businesses no longer trust the government or become nervous that helping maintain national security will lead to an avalanche of costly litigation, their cooperation will come to a grinding halt. Congress needs to take steps to retain the private sector's trust.

—Jena Baker McNeill is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.