Don't Shoot the Messenger: Telecommunications Carriers Deserve Immunity

BY JULIE A. HEDLUND | NOVEMBER 2007

It was the U.S. Department of Justice–and by extension, the Bush Administration–that gave legal assurances to the telecommunications carriers to justify their requests for information. If legal assurances from the highest levels of government were not valid, then the Administration is to blame, not the telecommunications carriers.

Many people are concerned about the federal government's activities to monitor Americans' telephone calls and e-mail messages. After 9/11, several telecommunications carriers complied with the federal government's requests for data. Now these companies are facing more than 40 lawsuits from individuals who claim their calls were tapped illegally and are demanding potentially billions of dollars in damages. Yet, the focus of our concern should not be on companies who complied with the government's requests. Rather, it should be on the Bush Administration, which implemented the program without Congressional approval or oversight.

Yet, in its legislation to overhaul the Foreign Intelligence Surveillance Act (FISA), Congress is poised to condone lawsuits against telecommunications carriers for complying with what they thought was a legal information-sharing program that was approved by the highest levels of government. In the wake of 9/11 the Bush Administration began to conduct emergency surveillance of the communications of suspected foreign terrorists in and out of the United States. Under this surveillance program, the government asked the country's major telecommunications carriers to allow the National Security Agency and law enforcement agents to conduct wiretaps and gather information without a warrant.

Believing that the federal government's requests were legal, several telecommunications carriers complied with them. Congress extended its oversight of the Bush Administration's post-9/11 emergency surveillance program when it learned of the program in 2006. Yet, public disclosure spurred numerous class-action lawsuits against the telecommunications carriers alleging that they violated the law when they complied with these requests.

As Congress considers reforms of FISA, two key points should be considered. First, the Bush Administration was wrong in not working with Congress from the beginning in implementing its post-9/11 emergency surveillance program. A change in national policy of this magnitude should have been made with the collaboration and oversight of Congress. Second, Congress is right to

consider updating FISA. Since FISA took effect in the 1970s, there have been dramatic changes not only in communications technology but also in the threats to national security. Unfortunately, however, much of the focus of the current debate has been not about how to revise the law but about whether telecommunications carriers who complied with the government's post 9/11 surveillance program should be sued for doing what they believed was complying with a legal government order.

Congress should not force a private company to make national security decisions that rightly belong to the government.

It's not as if the government does not already ask companies to provide a variety of sensitive data on many Americans in order to avert terrorist activities. Each day, U.S. law enforcement and national security agencies obtain personal information about thousands of U.S. citizens, including names, addresses, credit card information, and travel plans. They use these data to track potential terrorists. But the majority, if not all, of these U.S. citizens are not terrorists–they are airline passengers flying from Europe to the United States. The U.S.-European Union Passenger Data Agreement of 2006 requires airlines to provide this information for every flight into the United States from Europe. The tragedy of 9/11 provided the impetous for this historic data-sharing agreement and most people probably feel safer knowing that it may avert similar disasters.

Opponents of granting the telecommunication carriers immunity–including the Electronic Frontier Foundation and the American Civil Liberties Union, which are supporting many of the lawsuits against telecommunications carriers–argue that it is for the courts to decide whether these companies broke the law and, if so, what damages apply. Yet, it was the U.S. Department of Justice–and by extension, the Bush Administration–that gave legal assurances to the telecommunications carriers to justify their requests for information.

If legal assurances from the highest levels of government were not valid, then the Administration is to blame, not the telecommunications carriers. The various FISA bills in the Senate and the House already include important provisions to strengthen oversight of the government's post-9/11 surveillance program. Allowing lawsuits to go forward against the telecommunications carriers for supplying information under the program has the potential to impair future efforts by law enforcement to intercept terrorist communications under FISA. In addition, it will place a significant cost on the telecommunications companies that ultimately would be borne by their ratepayers.

Opponents of immunity also suggest that the telecommunications companies' lawyers could have reviewed the legality of the government's wiretapping requests. There are two problems with this argument. First, Congress should not force a private company to make national security decisions that rightly belong to the government. Company lawyers may not have the expertise to determine the legality of the government's terrorist surveillance program. Second, Congress should not expect a company to refuse a request from the highest levels of government. A representative of at least one company, Qwest, has argued that the Bush Administration retaliated against it by not giving it contracts because it refused to cooperate. Although there may be no basis for this claim, it would not be unreasonable for companies that refused to comply with the government's requests for information to fear increased regulatory scrutiny or other penalties. Adding this factor on top of their national patriotism explains why most companies decided they had no choice but to comply.

Some opponents of immunity have suggested another option that would let telecommunications carriers avoid paying extensive damage awards–namely, indemnification. The Senate Judiciary Committee's ranking Republican, Senator Arlen Specter, for example, favors a legislative provision that would grant telecommunications carriers indemnification while also placing a $1 billion cap on the U.S. government's liability. One problem with this proposal is that it would allow the lawsuits against telecommunications companies to go forward, requiring them to engage in prolonged and costly litigation to defend their actions. If the lawsuits go forward, telecommunications carriers, as well as other industries handling information of critical im-

portance to protecting the homeland, will be less likely to cooperate with the government's requests for information, even legitimate ones, in the future.

A second problem with this proposal is that it would force U.S. taxpayers to pay a windfall to people who believe their communications were compromised. Thus, if, as some allege, the government reviewed every American's communications under its surveillance program, then every American would be eligible to join one of these class-action lawsuits. The ridiculous result would be Americans getting awards that they pay for through their federal taxes. The only winners in this scenario would be trial lawyers.

A better approach is the bill voted out of the Senate Intelligence Committee last month that would provide telecommunications carriers with immunity. After reviewing classified White House documents on the government's warrantless surveillance program, Senator Rockefeller (D-WA) proposed legislation that would end current litigation and let the U.S. attorney general block courts or state public utility commissions from reviewing whether the government's wiretap requests violated state or federal laws. This bill would terminate cases brought by plaintiffs seeking monetary damages or a court ruling that the telecommunications carriers' actions were illegal. Yet, the bill has important restrictions and would not provide "blanket immunity" as some opponents have suggested. In particular, it would limit immunity to telecommunications companies that either did not do what plaintiffs claim or whose actions were based on assurances from officials at the highest levels of government that the President authorized the request and that it was legal. These restrictions are important because they make it clear that telecommunications carriers should not be penalized for obeying a law that they had every reason to believe was legal.

Telecommunications carriers that participated in the Bush Administration's post-9/11 emergency surveillance program were doing what they thought was their legal and patriotic duty. To do anything else would have been to defy the law of the land, the U.S. attorney general, and the President. To expect such defiance is simply not reasonable. The focus should be on oversight and accountability for the actions of the Bush Administration, not punishing telecommunications companies and U.S. taxpayers.

ABOUT THE AUTHOR

Julie Hedlund is a Senior Analyst with the Information Technology and Innovation Foundation (ITIF). She has advised IT companies and regulators concerning telecommunications and Internet policy and teaches a popular course for private and public sector officials from developing countries on Internet Regulatory and Trade Policy at the U.S. Telecommunications Training Institute in Washington, DC. She is co-author, with Dr. Robert D. Atkinson, on the ITIF report, "The Rise of the New Mercantilists: Unfair Trade Practices in the Innovation Economy," and author of the ITIF report, "Patents Pending: Patent Reform for the Innovation Economy."

ACKNOWLEDGEMENTS

The author wishes to thank Rob Atkinson, President, ITIF for his significant contributions.

ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.innovationpolicy.org.
ITIF | 1250 I St. N.W. | Suite 200 | Washington, DC 20005