900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org
Computer & Communications Industry Association

ABSTRACT

GOVERNMENT SURVEILLANCE / FISA

May 2008

- *Industry and its customers alike are affected negatively when information technology (IT) is deputized for undue intrusions into the communications of private individuals.*
- *CCIA strongly supports basic Fourth Amendment protections against undue search and seizure and opposes efforts to further erode civil liberties.*
- *Updating the Foreign Intelligence Surveillance Act (FISA) should not be held hostage to demands by phone companies for retroactive immunity.*

Background: The Foreign Intelligence Surveillance Act (FISA) was passed in 1978 and is intended to protect our national security and balance the privacy and civil liberties of Americans engaged in telephone or electronic communications. The attacks of Sept. 11, 2001 changed U.S. society in profound ways. Unfortunately, the legislative response embodied in the Protect America Act (PAA), which was rushed through Congress in August of 2007, swept away numerous restraints on law enforcement. It gutted privacy protections and inserted new undefined terms and loopholes that could be exploited by overzealous executive branch officials. Telephone companies who were asked for assistance with surveillance in tracking terrorists not only complied in the aftermath of 9-11 but also continued to participate in warrantless government wiretapping programs for many years thereafter, quite possibly in violation of FISA.

The White House eventually claimed that the President has the unilateral power to order surveillance of anyone suspected of being involved in activities that threaten national security. The Bush Administration has also insisted on retroactive immunity for companies that collaborated in warrantless electronic surveillance.

CCIA's Position: The mere possibility of widespread, secret, and unchecked surveillance of the billions of messages that flow among our customers, and U.S. citizens in particular, will erode the fundamental openness and freedom of our communications networks. Even if this power is not deliberately misused, the loss of privacy in personal and confidential business communications will inflict great and long lasting damage on the dynamic and innovative growth intrinsic to the high technology sector. Current legislation need not sacrifice privacy for national security nor compromise security in the name of civil liberties. Both the House of Representatives and the Senate Judiciary Committee passed important FISA improvements, which are being held hostage by the immunity issue.

The assertions that companies without retroactive immunity will not co-operate with a U.S. Administration's lawful requests for assistance are outrageous and false. There's just as much evidence to prove that companies will be good citizens and cooperate with intelligence agencies

as authorized by law to do so. That is why industry supports new legislation to further clarify FISA standards and procedures.

All agree that the current limited prospective immunity rules should be extended. Meanwhile, if the government can "paper over" past violations of FISA, no current restraint on government power can be relied upon, since the Administration will always be able to coerce companies into illegal acts in the name of national security by promising to again extend immunity for any crimes committed at the request of the government. A bipartisan team of judiciary experts should deal with the current retroactive immunity question separately.

No one knows the extent of the domestic spying program from 2001-2006, and we may never know if the litigation involving the telephone companies is not allowed to proceed at all, even with limitations on damages and closed courtroom rules.

A commitment to openness and growth in electronic commerce cannot be sustained if end users fear a betrayal of the privacy and security of their personal and business communications.
Our industry is confronted with escalating monitoring and surveillance by repressive foreign regimes. The U.S. government should lead in promoting freedom within repressive regimes. But such leadership will fall flat if all we can show is that our own surveillance is somewhat less pervasive. A failure to protect basic freedoms now can only weaken the hand of U.S. companies that must contend with censors, regulators and secret police abroad.

Key Players: In November 2007, the House of Representatives passed the RESTORE Act, H.R. 3773, which took a more balanced approach at addressing these issues. Speaker Nancy Pelosi herself took to the House floor in support of the RESTORE Act and explained the absence of special retroactive immunity for telephone companies. Legislators cited CCIA's opposition to immunity, which highlighted the fact that businesses in general did not support retroactive immunity. The Senate Select Committee on Intelligence also reported a bill, S.2248, that makes improvements in the PAA, such as increasing the role of the FISA Court and oversight by the Inspector General, but that bill also contained the controversial telecom immunity provision. The Senate Judiciary Committee then passed a version of the bill without the provision. Senators Whitehouse (D-RI) a former state Attorney General, Specter (R-PA) and Feinstein (D-CA) were very active in crafting difficult compromises over FISA amendments. Senator Chris Dodd (D-CT) spoke strenuously against "amnesty" for the phone companies on the Senate floor, as did many others, including Senator Richard Durbin (D-IL).

On February 10, the Senate passed S.2448 with the retroactive immunity provisions.

Current Status: The FISA bill currently faces a fierce partisan standoff, with the immunity issue at the center of the debate. The House Democratic leadership is trying to pass a new compromise bill that authorizes the government's intelligence agencies to appropriately expand their surveillance activities to aid anti-terrorist efforts, when certain core standards are met. The Bush Administration vows to veto any FISA bill that does not contain retroactive immunity for the telephone companies. That means that protection of private corporate interests is trumping both national security and civil liberties.

Update on Related Issue: Data Mining

The Federal Agency Data Mining Act (S. 236), originally sponsored by Senators, Feingold, Leahy, Sununu and Akaka requires that agencies of the federal government report to Congress and the public on the nature of all "data mining" activities. This includes projects that scour government and commercial databases in order to find patterns that might indicate criminal or other suspicious activity. The bill mandates a description of all information being gathered and the intended uses, as well as its likely effect on civil liberties. It also requires policies to protect the privacy and due process rights of individuals including requirements that information be collected and handled accurately. These Federal Agency Data Mining provisions were passed by the Senate as an amendment to S.4, which implements the recommendations of the 9/11 Commission. After conferencing with HR 1, these federal data mining provisions were signed into law last August.