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 2009

- *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.*
- *CCIA wants the new administration to uncover the extent of the US electronic spying program from 2001-2006 and to monitor the impact of Congress passing the Foreign Intelligence Surveillance Act (FISA) in 2008 with retroactive immunity for telecom companies. It sets a dangerous precedent in a democracy when a government acts ahead of the law and encourages companies to cooperate in exchange for promised immunity later.*
- *S. 773 and S. 778 are too broad and vague in defining what cyber security emergencies would warrant the closing down of private networks by the federal government. CCIA also sees danger in giving top government officials additional powers to monitor private and public networks without regard to privacy laws.*

Background: The Foreign Intelligence Surveillance Act (FISA) was passed in 1978. Its intention is 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. Parts of the Patriot Act are up for renewal in December 2009.

Telephone companies who were asked for assistance with electronic 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 and pushed for Congress to update FISA to include retroactive immunity for the telephone companies that cooperated. In 2008, Congress approved a renewal of FISA with retroactive immunity for major carriers who were facing 40 lawsuits for turning over customer records to the government without warrants.

In October 2008, the New York Times reported that the National Security Agency was eavesdropping on the private phone conversations of U.S. citizens overseas. Previously

President Bush and American intelligence officials had denied they were regularly spying on the calls of US soldiers, journalists, and aid workers stationed abroad. Whistleblowers said the eavesdropping continued even when it was obvious they were not monitoring for terrorist related material for security reasons and that workers at the NSA facility in Fort Gordon, Georgia, regularly shared phone sex excerpts from the tapes.

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 broadband Internet and the high technology sector. Legislation need not sacrifice privacy for national security, nor compromise security in the name of civil liberties.

Assertions that companies without retroactive immunity would not cooperate with a U.S. Administration's lawful requests for assistance are outrageous and false. There is equal evidence to prove that companies will cooperate with intelligence agencies within the law. All agree on limited prospective immunity rules. Meanwhile, if the government can "paper over" past violations of FISA, no current restraint on government power can be relied upon; 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. 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, 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 made 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 later passed a version of the bill without the provision. Senators Whitehouse (D-RI), a former state Attorney General, Specter (D-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). Dodd along with Sen. Russ Feingold (D-WI), also threatened a filibuster and used procedural roadblocks to delay floor action during the first half of 2008. Sen. John Rockefeller (D-WV) worked to reach a compromise agreement to bring the bill for a floor vote.

On July 10, 2008, former President Bush signed the FISA bill reauthorizing U.S. spying laws with retroactive immunity to telecommunications companies that turned over customer records to the government.

Current Status: President Obama, when he was still a senator, had concerns about passing FISA with retroactive immunity for the telecoms that cooperated with the government without warrants, but ultimately supported it. Even though Congress passed legislation in 2008 granting telecoms retroactive immunity, the nearly 40 pending lawsuits have been transferred to San Francisco where Chief U.S. District Judge Vaughn Walker is reviewing a constitutional challenge to the updated spying law passed by Congress. So far the Obama administration has filed papers in that case asking the judge to not require the disclosure sought by the plaintiffs in a case against AT&T, arguing that disclosing the information would reveal secrets about the government's program to detect and prevent terrorist attacks.

The Obama administration has also asked Judge Walker to dismiss a second lawsuit filed in September 2008 by AT&T customers that named only the government as a defendant in an effort to get around the telecom immunity provision in the bill and find out to what extent the government has spied on Americans without warrants. The new administration was criticized by bloggers for arguing that the executive branch is completely immune from litigation on illegal spying. A DOJ spokesman said the Obama administration is defending telecom immunity as it is currently the law, and it would also protect national security information. The DOJ, however, is reviewing spying and torture polices of the Bush administration.

In April 2009, Senators Rockefeller (D-WV) and Snow (R-ME) introduced S. 773 and S. 778, the Cybersecurity Act of 2009, and legislation to create a White House cybersecurity czar. The new Office of the National Cybersecurity Advisor would have broad new powers to monitor and control the Internet to protect this critical infrastructure from threats. The president would have the ability to declare a cyber security emergency and block or limit Internet traffic in any critical information network, including private ones, in the interest of national security. To do this, the Commerce Secretary would be given additional power to monitor private and public networks regardless of privacy laws.