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 2010

- *Industry and consumers are affected negatively when information technology (IT) is employed 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 urges the Obama 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. FISA 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.*

Background: The Foreign Intelligence Surveillance Act (FISA) was passed in 1978 and is intended to protect our national security while safeguarding the privacy and civil liberties of Americans engaged in telephone or electronic communications. The legislative response to the profound events of September 11, 2001 is embodied in the Protect America Act (PAA), which was rushed through Congress in August of 2007 and 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. Additionally, parts of the USA PATRIOT ACT were up for renewal in December 2009 and passed.

In the aftermath of 9-11, telephone companies were asked for assistance with electronic surveillance in the tracking of terrorists. The companies not only complied, but also continued to participate in warrantless government wiretapping programs for many years thereafter and, arguably, in violation of FISA. The Bush 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 facing lawsuits for turning over customer records to the government without warrants.

In October 2008, the New York Times reported that the National Security Agency (NSA) was eavesdropping on the private phone conversations of US citizens overseas. President Bush and American intelligence officials had previously denied regularly spying on the calls of US soldiers, journalists and aid workers stationed abroad.

CCIA's Position: The mere possibility of widespread, secret, and unchecked surveillance of the billions of messages that flow through networks, used primarily by U.S. citizens, will erode the

fundamental openness and freedom of our communications networks. Even if this power is not deliberately abused, 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 sufficient evidence to prove that companies would act as good citizens and cooperate with intelligence agencies when authorized by law to do so. 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.

A commitment to Internet openness and growth in electronic commerce cannot be sustained if end users fear a betrayal of their privacy and security. Our industry is confronted with escalating monitoring and surveillance by repressive foreign regimes. The U.S. government should lead in promoting freedom within these regimes, but such leadership won't work if we are engaging in the same activity without due process. Failure to protect basic privacy and civil liberties at home weakens 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 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 the business community 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 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.). Dodd, along with Sen. Russ Feingold, D-Wis., also threatened a filibuster and used procedural roadblocks to delay floor action during the first half of 2008. Sen. John Rockefeller, D-WVa. also worked to reach a compromise agreement.

President Bush signed the FISA bill in July 2008, which reauthorized U.S. spying laws and provided retroactive immunity to telecommunications companies that turned over customer records to the government.

Current Status: Even though Congress passed legislation in 2008 granting telecoms retroactive immunity, the nearly 40 pending lawsuits were transferred to San Francisco where Chief US District Judge Vaughn Walker is reviewing a constitutional challenge to the updated spying law passed by Congress. The Obama administration has filed papers in the 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 Department of Justice spokesman said the Obama administration is defending the current telecom immunity measure, as it protects national security information.

In January 2010, a federal judge in San Francisco dismissed Jewel v. NSA, filed by the Electronic Frontier Foundation (EFF) on behalf of AT&T customers, which challenged the surveillance of millions of Americans' phone calls and emails. EFF said it plans to appeal. EFF had offered evidence, which AT&T did not dispute, that AT&T routed its customers' electronic traffic to San Francisco so it could be routinely examined by NSA.

In September 2009, CCIA wrote a letter thanking Sen. Richard Durbin, D-Ill., for introducing legislation to repeal the retroactive immunity provision in the FISA Amendments Act.

In February 2010, the Senate voted to renew the USA PATRIOT Act, which included provisions to allow wiretapping and surveillance that would have otherwise expired. Judiciary Chairman Patrick Leahy said he wished he could have added better oversight and review measures to the bill.