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

NATIONAL SECURITY / FISA

May 2011

- *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 PATRIOT Act of 2001 and the Protect America Act (PAA) of 2007, both of which were rushed through Congress and swept away numerous restraints on law enforcement. They gutted privacy protections and inserted new undefined terms and loopholes that could be exploited by overzealous executive branch officials.

In the aftermath of September 11th, telephone companies were also 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. 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.

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 this retroactive immunity for major carriers facing lawsuits for turning over customer records to the government without warrants.

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. All the evidence shows that companies will act as good citizens and cooperate with intelligence agencies when authorized by law to do so. 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.

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 promote the privacy and free flow of information globally, 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 and secret police abroad.

Key Players: In February 2011, conservative tea party members of the House Republican Caucus gave the majority leaders an embarrassing shock when they voted with many Democrats against an extension of the PATRIOT Act on a suspension of the rules. While the extension later passed under a rule, the event showed that not all of the new Republican freshman members were going to support a system that threated civil liberties.

By and large, however, the discussion over national security, FISA, and warrantless wiretapping has moved to the courts, instead of the legislature. Judge Walker in the Northern District of California holds a docket of consolidated cases surrounding the warrantless wiretapping issue, and the Ninth Circuit Court of Appeals is currently reviewing one of his decisions. The Electronic Frontier Foundation and the American Civil Liberties Union are involved in the cases against the government and AT&T.

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 constitutional challenges to the updated spying law passed by Congress and to the original wiretapping. The Obama administration has filed motions in these cases asking the judge to dismiss the claims and not to require the disclosure sought by the plaintiffs, arguing that disclosure would reveal secrets about the government's efforts to protect national security. In January 2010, Judge Walker dismissed one case, Jewel v. NSA, but did so on grounds that the plaintiffs lacked standing. EFF has filed an appeal with the Ninth Circuit Court of Appeals.

In February 2011, the House voted on a bill to extend the USA PATRIOT Act through the end of the year. Speaker Boehner originally brought the bill up on a suspension of the rules, but the measure failed to gain the 2/3 majority required under that rule. It was later brought up under the regular rules and passed. A bill in the Senate was also passed to extend the law for three months, however, and this bill is what eventually passed both chambers. The Congress will have to vote again by May 27th if it is to extend the provisions again.