

## AT&T WHISTLEBLOWER MARK KLEIN: Reject Amnesty for Telecoms

For about five years, the Bush administration's National Security Agency, with the help of the country's largest telecommunications companies, has been collecting your email, accumulating information on your web browsing, and gathering details about your Internet activity, all without warrants and in violation of the U.S. Constitution and several federal and state laws. Even after the program was exposed by *The New York Times* in December 2005 President Bush and other government officials consistently defended the NSA's activities, insisting that the NSA only collects communications into or from the United States where one party to the communication is someone they believe to be a member of al Qaeda or an associated terrorist organization.

But these claims are not true. I know they are not true because I have first-hand knowledge of the clandestine collaboration between one giant telecommunications company and the NSA to facilitate the most comprehensive spying program in history. I have seen the NSA's vacuum cleaner surveillance infrastructure with my own eyes. It is a vast, government-sponsored warrantless spying program.

For over 22 years, I worked as a technician for AT&T. While working in San Francisco in 2002, I learned that a management-level technician, with AT&T's knowledge, had been cleared by the NSA to work on a special but secret project: the installation and maintenance of Internet equipment in a newly-constructed, secure room in AT&T's central office in San Francisco. Other than the NSA-cleared technician, no employees were allowed in that room. In October 2003 I was transferred to that office, and was in particular assigned to oversee AT&T's Internet operations.

As part of my duties, I was required to connect circuits carrying Internet data to optical "splitters," which made a copy of the light signal. But the "splitters" weakened the light signal, causing problems I had to troubleshoot. After examining engineering documents given to the technicians which showed the connections of the splitters, I discovered that they were hard-wired to the secret NSA room.

In short, an exact copy of all Internet traffic that flowed through critical AT&T cables—emails, documents, pictures, web browsing, Voice-Over-Internet phone conversations, everything—was being diverted to equipment inside the secret room. In addition the documents reveal the technological gear used in their secret project, including a highly-sophisticated search component capable of quickly sifting through huge amounts of digital data (including text, voice and images) in real time according to pre-programmed criteria.



**Mark Klein** is a former AT&T telecommunications technician who has come forward to provide evidence of the company's illegal collaboration with the NSA.

It's important to understand that the Internet links which were connected to the splitter contained not just foreign communications but vast amounts of domestic traffic, all mixed together. Furthermore, the splitter has no selective abilities—it's just a dumb device which copies everything to the secret room. And the links going through the splitter are AT&T's physical connections to many other Internet providers (e.g., Sprint, Qwest, Global Crossing, Cable & Wireless, and the critical West Coast Internet Exchange Point known as Mae West). Since these networks are interconnected, the government surveillance affects not only AT&T customers but everyone else—millions of Americans.

I also discovered in my conversations with other technicians that other “secret rooms” were established in Seattle, San Jose, Los Angeles and San Diego. One of the documents I obtained also mentions Atlanta, and the clear inference in the logic of this setup, and the language of the documents, is that there are other such rooms across the country to complete the coverage—possibly 15 to 20 or more.

So when reports of the government's extensive wiretapping program surfaced in December 2005, after I had left AT&T, I realized two things: First, that I had been a witness to a massive spying effort that violated the rights of millions of Americans; and second, that the government was not telling the public the truth about the extent of their unconstitutional invasion of privacy. In the spring of 2006 I became a witness for the Electronic Frontier Foundation's lawsuit against AT&T. And the New York Times (April 13, 2006) reported that four independent technical experts who examined the AT&T documents “all said that the documents showed that AT&T had an agreement with the federal government to systematically gather information flowing on the Internet.”

Congress has not had aggressive investigations into what the government is doing: subpoenas have been ignored by the administration, which has so far succeeded in keeping most everything a secret from the American people, except for revelations in the media. Given the administration's years-long record of misdirection and outright prevarication, it would only be playing into their hands to give them what they want on the basis of “trust me” statements.

But that is exactly what was done with the law passed hurriedly by Congress in August, which gave the administration virtually everything they wanted including immunity for the telecoms going forward. Now the telecom lobbyists and the administration are back to get the final piece, i.e., retroactive immunity for the telecoms. But the lawsuits brought by EFF and many others remain the last best chance to find out exactly what's been going on. Amnesty would represent both an outrageous short-circuiting of the judicial process by Congress and, frankly, an outright cover-up of crimes.

Congress is now debating a new bill allegedly to correct the egregious August giveaway. I don't want to get into the minutiae of the various versions, except to note that the proposal for so-called “basket warrants” is just another name for the well-hated “general warrants” banned by the Fourth Amendment of the Constitution. A far better way to undo the dangerous spying agenda of this administration would be to physically rip out the “secret rooms” illegally installed in AT&T's network.

But most immediately, Congress must not give retroactive immunity to the telecoms or to administration officials. That would only compound the many crimes already committed.

**Electronic Frontier Foundation** [www.eff.org](http://www.eff.org)  
Contacts: Kevin Bankston of EFF at (415) 748-8126 or Adam Eisgrau (202) 215-6884