Lawsuit details AT&T cooperation in illegal government spying on Americans

Joe Kay
18 April 2006

A lawsuit underway in a US district court in San Francisco charges telecommunications giant AT&T with violating the privacy of its customers by handing over massive amounts of data to the government. The class action lawsuit, filed by the Electronic Frontier Foundation on behalf of AT&T customers, is based on documents provided by a former AT&T employee that detail the company's participation in the National Security Agency (NSA) warrantless spying program that was first revealed late last year.

The documents, obtained by Mark Klein, a former technician at AT&T, are currently under court seal. They were provided to the *New York Times* by Klein, who also released a statement earlier this month describing what he discovered while working at the company. AT&T has filed a motion to have all the documents returned on the grounds that they are proprietary, but the company has not denied the validity of the documents or Klein's statements.

If true, Klein's statements confirm that the spying carried out by the NSA is much broader than has been acknowledged by the government, and has been made possible only through the willing participation of a handful of giant corporations in the US. The NSA program involves a direct violation of the 1978 Foreign Intelligence Surveillance Act, as well as provisions of the Bill of Rights that prohibit unwarranted search and seizure.

Klein's revelations strongly suggest a criminal conspiracy between a section of corporate America and the US government.

According to a *New York Times* article published on April 13, the documents, which the newspaper handed over for examination by four telecommunications and computer security experts, "describe equipment capable of monitoring a large quantity of e-mail messages, Internet phone calls, and other Internet traffic" The equipment "was able to select messages that could be identified by keywords, Internet or e-mail addresses or country of origin and divert copies to another location for further analysis."

"The technical experts," the *Times* reported, "all said the documents showed that AT&T had an agreement with the federal government to systematically gather information flowing on the Internet through the company's network."

In a statement released by his lawyers, Klein said that the equipment was installed in a secret room in an AT&T facility in San Francisco, where Klein worked for 23 years before leaving in 2004. Ordinary employees at the company were not allowed access to the room, which was adjacent to the "switches" through which data and phone calls are routed. Klein said that cables connected the switches with the room operated at the behest of the NSA, allowing the government free rein to monitor all communications.

"Based on my understanding of the connections and equipment at issue," Klein said, "it appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the Internet—whether that be people's e-mail, Web surfing or any other data."

In addition to the room in San Francisco, Klein said he also learned of a similar facility at an AT&T switching location in Atlanta. The documents cited by the *Times* indicated that the cooperation extended to facilities in San Jose, San Diego and Los Angeles, California; and Seattle, Washington. These hubs channeled e-mails and other data from a large number of other Internet providers to AT&T, meaning that the number of people potentially spied on extends well beyond AT&T's customer base.

The data to which the government has access is not limited to these cities, since the facility Klein worked at was connected "with other networks and hence the whole country, as well as the rest of the world."

Previous reports have indicated that a number of other companies have participated in a similar way, though details have not emerged of the extent of participation of these companies.

There is nothing in the technology involved that would limit the government to monitoring communications going into and out of the United States, despite the claims of the Bush administration that only such communications are being targeted by the NSA. According to the *Times*, "The network designer and other experts said it would be a simple technical matter to reprogram the equipment to intercept purely domestic Internet traffic." The only guarantee that this has not already happened is the word of the American government.

The statements by Klein and the documents obtained by the *Times* directly contradict previous assertions by the Bush administration that the spying program is limited in scope. For example, Michael Hayden, the principle deputy director of national intelligence and former director of the NSA, declared in a speech on January 23 that the NSA program is not a "driftnet" monitoring conversations "that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about." In fact, according to Klein, this is precisely what the program involves.

In response to the recent revelations, the government has given its standard response: It refuses to talk about "operational details," while suggesting that any attempt to expose its violation of the democratic rights of the American people amounts to support for terrorism. "Any discussion about actual or alleged operational issues would be irresponsible as it would give our adversaries insight that would enable them to adjust and potentially inflict harm to the US," remarked NSA spokesman Don Weber. An AT&T spokesman stated that the company is "not in a position to comment on matters of national security or litigation."

While publicly stating that the NSA warrantless spying program is limited to international calls targeting Al Qaeda suspects, the administration has been careful not to imply that it is legally constrained from engaging in something much broader. On April 6, Attorney General Alberto Gonzales told a Senate panel that he would not rule out government authority to monitor purely domestic calls and other communications if this was necessary for the "war on terrorism."

In a letter in late February, Gonzales noted that in remarks to the Senate that month in which he denied that the government was spying on purely domestic communications he "did not and could not address...any other classified intelligence activities" beyond what had been admitted by the government. Russell Tice, a former NSA employee, has said that the agency has authorization to engage in much broader spying as part of a top-secret "special access program."

The logic of the administration's argument is that it has the unlimited power to spy on anyone, including US citizens, as part of the supposed commander-in-chief authority of the president. The same justification has been used by the administration to justify arbitrary and indefinite detention, torture and other violations of basic democratic principles.

Only a few months after it was initially exposed late last year, the government's warrantless domestic spying program has largely been dropped by both the news media and the Democratic Party. A proposed investigation was scuttled by the Senate Intelligence Committee in March. At the end of March, a proposal to censure Bush for violating the law by authorizing the NSA program received virtually no support from either party.

Whatever the extent of the current spying, the precedent set is absolutely clear: American big business is perfectly willing to aid the government in violating the democratic rights of the American people, and there will be no serious opposition from within the political establishment.