

Whistle-Blower Out's NSA Spy Room

By [Ryan Singel](#) | [Also by this reporter](#)

11:15 AM Apr, 07, 2006

AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, according to a former AT&T worker cooperating in the Electronic Frontier Foundation's lawsuit against the company.

Mark Klein, a retired AT&T communications technician, submitted an affidavit in support of the EFF's lawsuit this week. That [class action](#) lawsuit, filed in federal court in San Francisco last January, alleges that AT&T violated federal and state laws by surreptitiously allowing the government to monitor phone and internet communications of AT&T customers without warrants.

On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching center in 2002 to interview a management-level technician for a special job. In January 2003, Klein observed a new room being built adjacent to the room housing AT&T's #4ESS switching equipment, which is responsible for routing long distance and international calls.

"I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room," Klein wrote. "The regular technician work force was not allowed in the room."

Klein's job eventually included connecting internet circuits to a splitting cabinet that led to the secret room. During the course of that work, he learned from a co-worker that similar cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

"While doing my job, I learned that fiber optic cables from the secret room were tapping into the Worldnet (AT&T's internet service) circuits by splitting off a portion of the light signal," Klein wrote.

The split circuits included traffic from peering links connecting to other internet backbone providers, meaning that AT&T was also diverting traffic routed from its network to or from other domestic and international providers, according to Klein's statement.

The secret room also included data-mining equipment called a Narus STA 6400, "known to be used particularly by government intelligence agencies because of its

ability to sift through large amounts of data looking for preprogrammed targets," according to Klein's statement.

[Narus](#), whose website touts AT&T as a client, sells software to help internet service providers and telecoms monitor and manage their networks, look for intrusions, and wiretap phone calls as mandated by federal law.

Klein said he came forward because he does not believe that the Bush administration is being truthful about the extent of its extrajudicial monitoring of Americans' communications.

"Despite what we are hearing, and considering the public track record of this administration, I simply do not believe their claims that the NSA's spying program is really limited to foreign communications or is otherwise consistent with the NSA's charter or with FISA," Klein's wrote. "And unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of internet communications of countless citizens."

After asking for a preview copy of the documents last week, the government did not object to the EFF filing the paper under seal, although the EFF asked the court Wednesday to make the documents public.

One of the documents is titled "Study Group 3, LGX/Splitter Wiring, San Francisco," and is dated 2002. The others are allegedly a design document instructing technicians how to wire up the taps, and a document that describes the equipment installed in the secret room.

In a letter to the EFF, AT&T objected to the filing of the documents in any manner, saying that they contain sensitive trade secrets and could be "could be used to 'hack' into the AT&T network, compromising its integrity."

According to court rules, AT&T has until Thursday to file a motion to keep the documents sealed. The government could also step in to the case and request that the documents not be made public, or even that the entire lawsuit be barred under the seldom-used [State Secrets Privilege](#).

AT&T spokesman Walt Sharp declined to comment on the allegations, citing a company policy of not commenting on litigation or matters of national security, but did say that "AT&T follows all laws following requests for assistance from government authorities."

Ads by Google

ESD Australia (TSCM) Specialist's in the detection of covert surveillance devices.
www.esd-australia.com

listening device
Looking for a new Hearing Aid?
Search here and save money!
www.hearing-aid-search.com

Business Voice recorder
Defuse lawsuits & correct errors
by recording business phone calls
www.versadial.com/

Iran Earthquake Relief
Help the 20k+ victims.
Your financial support will save lives.
www.niacouncil.org

Wired News: [Contact Us](#) | [Advertising](#) | [Subscribe](#)
We are translated daily into Korean and Japanese

© Copyright 2006, Lycos, Inc. All Rights Reserved.

Your use of this website constitutes acceptance of the Lycos [Privacy Policy](#)

