

EXHIBIT H



Text Size: A A A A

• Cars • Computers • Gadgets • Internet • Med-Tech • Security • Space • Software • Wireless


Court Deals AT&T a Setback

By Ryan Singel Also by this reporter


11:30 AM May, 17, 2006

SAN FRANCISCO -- A federal judge Wednesday shot down telecom giant AT&T's efforts to recover and suppress internal documents that a former AT&T technician says demonstrate the company's collusion in illegal government surveillance.

Inside the Secret Room



Courtroom Clash!
A federal judge refuses to give AT&T back its internal documents, but orders the EFF not to give them out.



Whistle-Blower's Precognition
Years before the NSA's warrantless surveillance program made national headlines, then-AT&T technician Mark Klein suspected his company was colluding with the government to spy on Americans.

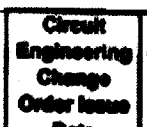


Exhibit A?
Former AT&T technician Mark Klein offers a firsthand account of his alleged discovery of a secret room routing American internet traffic straight to the NSA -- and provides documents he says prove his case.


The

The documents, portions of which were published Wednesday by Wired News, are Exhibit A in the Electronic Frontier Foundation's class-action lawsuit against AT&T. The EFF alleges that the company illegally turned over vast troves of phone-record data to the National Security Agency, and has wired its internet backbone to secret NSA surveillance equipment.


Last week the government formally asked U.S. District Judge Vaughn Walker to throw out the case for alleged national security reasons, a motion now scheduled to be heard June 23.

In the standing-room-only hearing Wednesday, the judge rejected the EFF's request that the documents provided to the organization by former company technician Mark Klein be unsealed in court records, and ordered EFF not to share the papers with anyone.

"It appears that there is a possibility that the



Ultimate Net Monitoring Tool
A little-known company called Narus makes the packet-inspection technology said to be the basis of the NSA's internet surveillance. Here's how it works.



Plus: Daily updates from 27B Stroke 6, the Wired News security and privacy blog.

documents contain significant trade secrets or proprietary information belonging to AT&T," said Walker.

But he rejected AT&T's motion asking the court to order EFF to return the documents to the company, noting, "Plaintiffs say they got the documents innocently, therefore, their possession is in no way improper and in no way illegal."

He also rejected AT&T's request for the judge to enjoin Klein from talking about the documents or providing them to others, saying that AT&T could sue the whistle-blower on its own.

The documents appear to show AT&T tapping into 16 fiber-optic cables connecting the company's WorldNet internet backbone to other internet service providers, and routing the traffic to a sophisticated data-analysis system made by California-based Narus.

In a written statement accompanying the pages, whistle-blower Klein says the Narus system was installed in a secret locked room inside an AT&T switching center in San Francisco that was off-limits to anyone without NSA clearance.

In court, AT&T attorney Bradford Berenson cast his client as a hapless victim, unable to defend itself while maintaining its national security obligations.

"The problem here is not just that the plaintiffs can't make their case, but that the defendants can't defend themselves," said Berenson, noting that some perfectly legal instruments of surveillance, like Patriot Act national security letters, come with binding secrecy requirements.

"AT&T is an innocent bystander, and the fight should be between private parties and the government that started these (surveillance) programs and ran them," Berenson told the court.

Walker made clear that he wants the case to move forward quickly -- so fast that EFF attorney Cindy Cohn resorted to begging for extra time to file

briefs.

One of those briefs is due Monday, advising the judge on how he should approach reading the government's classified arguments as to why the case should be dismissed.

The classified filing is currently in Washington, D.C., but can be flown under protective custody to San Francisco for the judge's inspection, according to Justice Department lawyer Carl Nichols.

Nichols told the judge that the extraordinary secrecy was necessary, because unlike a hypothetical case about the disclosure of a fighter jet weapon design -- where the government can admit the design exists -- "this case involves national intelligence sources and methods."

"To tell you those things in open court where they will be in the public record is to disclose the very thing we are trying to protect," Nichols said.

Walker asked some pointed and skeptical questions about whether the nearly all-powerful state secrets privilege, a holdover from English common law, trumps the Constitution and Congress.

"It is an inherent Article II (executive branch) power which unfortunately trumps a private litigant's right to his day in court," Nichols said.

Walker's ruling on the government's motion to dismiss the case for national security reasons could come as early as the June 23 hearing, but his ruling either way is nearly certain to trigger an immediate appeal to the 9th U.S. Circuit Court of Appeals.

That's one reason the EFF asked the judge to first hear its motion for a preliminary injunction since, as Cohn argued, the "massive flow of information will continue during the appeal."

Walker called that "putting the cart before the horse," and will first rule on the government's and AT&T's motions to dismiss the case.

After the hearing, Klein addressed reporters on the courthouse steps.

"As you all know there is a big public debate going on about government

surveillance," Klein said in a voice barely above a whisper. "I believe I have significant information to bring to the table, and I have been struggling for some time to bring it out in the light of day. And that's all I wanted to do -- is bring it out so that people can examine it and decide for themselves."

Editor's note: This story was updated at 12:30 p.m. and 2 p.m. to add additional information.

Ads by Google

Secretly Monitor Email
Remotely Spy on Chats,
Keystrokes,
and Passwords. Download
Instantly.
www.spyready.com

Digital Surveillance PROs
We manufacture systems
for business
Our Engineers Design
Systems Free!
www.rugged-cctv.com

Surveillance
Equipment
Helpful Links for
Surveillance
Equipment
www.ToSeekA.com

NetBotz Surveillance
Monitor Assets w/ IP-Based
Security
Solutions from NetBotz.
Learn More!
www.apcc.com

Wired News: [Contact Us](#) | [Advertising](#) | [Subscribe](#)

We are translated daily into Korean and Japanese

© Copyright 2006, Lycos, Inc. Lycos is a registered trademark of Lycos, Inc. All Rights Reserved.

Your use of this website constitutes acceptance of the Lycos

Privacy Policy and **Terms & Conditions**