EXHIBIT F

Stumbling Into a Spy Scandal

By Ryan Singel | Also by this reporter
02:00 AM May, 17, 2006

When former AT&T technician Mark Klein learned of a secret room installed in the company's San Francisco internet switching center, he was certain he had stumbled onto the Total Information Awareness program, a Defense Department research project that intended to scour databases across the country for telltale signs of terrorists.

Though the program had mostly been terminated by Congress in September 2003, portions of the program were allowed to continue.

Klein believed he had found these remnants, according to a written statement by Klein acquired by Wired News. AT&T built the secret room in 2003 and wired it up to receive a copy of the internet traffic running through its fiber-optic network, according to Klein's statement and accompanying documents. Inside the room, AT&T had installed routers, Sun Microsystems servers and traffic-analysis software from a company called Narus.

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

One of the documents appears to describe AT&T's successful efforts to tap into 16 fiber-optic cables connecting the company's WorldNet internet backbone to other internet service providers. The document shows AT&T technicians phasing in fiber-optic splitters throughout February 2003, cutting them in four at a time on a weekly schedule, ending with a link to Mae West, an internet exchange point for West Coast traffic.

"It's not just WorldNet customers who are being

technician Mark Klein suspected his company was colluding with the government to spy on Americans.

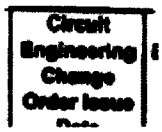

Exhibit A? Former AT&T technician Mark Klein offers a firsthand account of his alleged discovery of a secret room routing American internet traffic straight to the NSA -- and provides documents he says proves his case.

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

spied on," Klein wrote.

"The essential hardware elements of a (Total Information Awareness)-type spy program are being surreptitiously slipped into 'real world' telecommunications offices," Klein wrote, referring to "secret rooms" in central offices across the country that Klein believed contained "computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire internet."

At times, Klein comes across as unhappy with AT&T, making a pointed reference to company downsizing and grumbling about union workers being prohibited from working in the secret rooms.

In December 2005, following *The New York Times*' revelation -- and government confirmation -- that the National Security Agency was engaged in warrantless surveillance of Americans' overseas calls, and e-mails to and from people suspected of ties to al-Qaida, Klein revised his thesis.

"But now it's been revealed by *The New York Times* that the spying program is vastly bigger and was directly authorized by President Bush, as he himself has now admitted, in flagrant violation of specific statutes and constitutional protections for civil liberties," Klein wrote. "I am presenting this information to facilitate the dismantling of this dangerous Orwellian project."

Klein noted that only persons with a clearance from the NSA could enter this room.

Included in Klein's statement are snippets of wiring diagrams stamped "AT&T Proprietary," several photos of Room 641A in AT&T's switching center at 611 Folsom St., and copies of web pages showing that Narus had sponsored a 2003 conference where industry and law enforcement discussed internet surveillance and phone wiretapping.

Klein showed up at the Electronic Frontier Foundation unannounced in late January with documents in hand. At the time, the EFF was already preparing a class-action lawsuit against AT&T for allegedly turning over customer phone-record data to the NSA -- relying on reporting from the *Los Angeles Times* about AT&T giving the NSA access to a phone-record database with 1.88 trillion entries.

The EFF later filed an affidavit from Klein, along with the full wiring documents and an evaluation of those documents by a former FCC internet specialist, under temporary seal in U.S. District Court. AT&T has told the court it wants the documents returned, and both parties will argue their positions before U.S. District Court Judge Vaughn Walker in San Francisco on Wednesday.

Several high-level network experts who reviewed the documents, which Klein has provided to civil liberties groups and *The New York Times*, say the pages may not be the smoking gun that Klein believes them to be.

One network expert familiar with AT&T's internet operations suggests that Klein may have simply stumbled upon an effort to monitor internet traffic for security threats, abnormal traffic patterns and network-management issues.

He said technicians may not have known about these programs, which can be used to monitor AT&T's WorldNet internet traffic, as well as corporate networks administered by AT&T.

For example, the setup described in the documents largely resembles AT&T Internet Protect, a service that "provides valuable real-time analysis of internet traffic, which customers can use to predict and prevent malicious traffic from infecting their network," according to AT&T's website.

Steve Bellovin, a Columbia University computer science professor and a former AT&T researcher, says that the documents don't contradict Klein's accusation that this is an NSA-related operation, but they also don't prove the existence of widespread NSA internet monitoring, because the equipment could simply be building up a traffic matrix for internal network monitoring.

"AT&T is probably the top ISP for doing its own network analysis and

measurement," Bellovin said. "A lot of that monitoring is producing the internet equivalent of the call-detail-record databases that all the phone companies, except Qwest, are alleged to have given to NSA. This is the internet equivalent at the IP address level. If A is talking to B at the IP address level, this will show you connectivity patterns.

"Much of this stuff the documents describe is 100 percent innocent. The suspicious part is the business about security clearances rather than the equipment," Bellovin said.

A third networking researcher familiar with internet and telecommunications networks who spoke on condition of anonymity echoes Bellovin's analysis.

"What is clear from these documents is that all of the traffic going on the fiber-optics links is being copied into this other room," the researcher said. "The question is why would you want to do this? One obvious conclusion is you might want to do it to turn it over to government, but by themselves, these documents don't definitely say that is what happened. The other reason you might want to do something like this is for network monitoring.

"The much more interesting stuff is the Narus box," the researcher added. "That stuff is incredibly computationally powerful and can do kinds of filtering on very high-bandwidth traffic. That does make it very suitable for pushing NSA surveillance into the edges of the network so they can pick off the stuff they are interested in.

"The big unanswered question is what happens to that data," he said. The documents would be a smoking gun "if there were another picture in the diagram showing another fiber-optic link to Fort Meade (NSA's headquarters), but as far as I can tell that's not there."

For its part, Narus says it can't confirm or deny Klein's allegations. But AT&T is an announced customer, according to Steve Bannerman, Narus' vice president of marketing and product management.

Narus' traffic processing enables ISPs to monitor traffic for billing and service reasons, secure their networks and comply with lawful interception requirements such as the Communications Assistance for Law Enforcement Act, or CALEA.

The company also has little to no knowledge of how a customer uses or extends the software's functions.

"We take great pains to build into the product the ability to manage those warrants so you don't accidentally target a user for longer than the warrant specifies," Bannerman said. "However, once a user installs our product, it's completely opaque to us if they actually type in a warrant."

The EFF hopes Klein's statement, along with the full documents it has filed with the court, persuade the judge it has a good-faith reason to believe AT&T is violating the law. If the court agrees with EFF, and decides not to honor the government's request to dismiss the suit for national security reasons, EFF would be able to obtain further documents through the discovery process.

For its part, AT&T says it vigorously defends its customers' privacy, though it has not directly contradicted Klein's accusations.

"If and when AT&T is asked by government agencies for help, we do so strictly within the law and under the most stringent conditions," reads a statement released by AT&T. "Beyond that, we can't comment on matters of national security. This is a national security issue and needs to be addressed on a national level."

AT&T plans to ask that the courtroom be cleared of observers for Wednesday's 10 a.m. hearing, according to the EFF.