AT&T Whistle-Blower's Evidence

02:00 AM May, 17, 2006

Former AT&T technician Mark Klein is the key witness in the Electronic Frontier Foundation's class-action lawsuit against the company, which alleges that AT&T illegally cooperated in an illegal National Security Agency domestic-surveillance program.

In this recently surfaced statement, Klein details his discovery of an alleged surveillance operation in an AT&T office in San Francisco, and offers his interpretation of company documents that he believes support his case.

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.

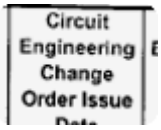

Exhibit A?
Former AT&T technician Mark Klein offers a firsthand account of his alleged discovery of a secret room routing American internet traffic straight to the NSA -- and provides documents he says proves his case.

The Ultimate Net Monitoring

For its part, AT&T is asking a federal judge to keep those documents out of court, and to order the EFF to return them to the company. Here Wired News presents Klein's statement in its entirety, along with select pages from the AT&T documents.

AT&T's Implementation of NSA Spying on American Citizens
31 December 2005

I wrote the following document in 2004 when it became clear to me that AT&T, at the behest of the National Security Agency, had illegally installed secret computer gear designed to spy on internet traffic. At the time I thought this was an outgrowth of the notorious Total Information Awareness program which was attacked by defenders of civil liberties. 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. I am presenting this information to facilitate the dismantling of this dangerous Orwellian project.

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

AT&T Deploys Government Spy Gear on WorldNet Network
-- 16 January, 2004

In 2003 AT&T built "secret rooms" hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire internet. These installations enable the government to look at every individual message on the internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities.

The physical arrangement, the timing of its construction, the government-imposed secrecy surrounding it, and other factors all strongly suggest that its origins are rooted in the Defense Department's Total Information Awareness (TIA) program which brought forth vigorous protests from defenders of constitutionally protected civil liberties last year:

> "As the director of the effort, Vice Adm. John M. Poindexter, has described the system in Pentagon documents and in speeches, it will provide intelligence analysts and law enforcement officials with instant access to information from internet mail and calling records to credit card and banking transactions and travel documents, without a search warrant." *The New York Times*, 9 November 2002

To mollify critics, the Defense Advanced Research Projects Agency (Darpa) spokesmen have repeatedly asserted that they are only conducting "research" using "artificial synthetic data" or information from "normal DOD intelligence channels" and hence there are "no U.S. citizen privacy implications" (Department of Defense, Office of the Inspector General report on TIA, December 12, 2003). They also changed the name of the program to "Terrorism Information Awareness" to make it more politically palatable. But feeling the heat, Congress made a big show of allegedly cutting off funding for TIA in late 2003, and the political fallout resulted in Adm. Poindexter's abrupt resignation last August. However, the fine print reveals that Congress eliminated funding only for "the majority of the TIA components," allowing several "components" to continue (DOD, *ibid*). The essential hardware elements of a TIA-type spy program are being surreptitiously slipped into "real world" telecommunications offices.

In San Francisco the "secret room" is Room 641A at 611 Folsom Street, the site of a large SBC phone building, three floors of which are occupied by AT&T. High-speed fiber-optic circuits come in on the 8th floor and run down to the 7th

floor where they connect to routers for AT&T's WorldNet service, part of the latter's vital "Common Backbone." In order to snoop on these circuits, a special cabinet was installed and cabled to the "secret room" on the 6th floor to monitor the information going through the circuits. (The location code of the cabinet is 070177.04, which denotes the 7th floor, aisle 177 and bay 04.) The "secret room" itself is roughly 24-by-48 feet, containing perhaps a dozen cabinets including such equipment as Sun servers and two Juniper routers, plus an industrial-size air conditioner.

The normal work force of unionized technicians in the office are forbidden to enter the "secret room," which has a special combination lock on the main door. The telltale sign of an illicit government spy operation is the fact that *only people with security clearance from the National Security Agency can enter this room.* In practice this has meant that only one management-level technician works in there. Ironically, the one who set up the room was laid off in late 2003 in one of the company's endless "downsizings," but he was quickly replaced by another.

Plans for the "secret room" were fully drawn up by December 2002, curiously only four months after Darpa started awarding contracts for TIA. One 60-page document, identified as coming from "AT&T Labs Connectivity & Net Services" and authored by the labs' consultant Mathew F. Casamassima, is titled *Study Group 3, LGX/Splitter Wiring, San Francisco* and dated 12/10/02. (See sample PDF 1-4.) This document addresses the special problem of trying to spy on fiber-optic circuits. Unlike copper wire circuits which emit electromagnetic fields that can be tapped into without disturbing the circuits, fiber-optic circuits do not "leak" their light signals. In order to monitor such communications, one has to physically cut into the fiber somehow and divert a portion of the light signal to see the information.

This problem is solved with "splitters" which literally split off a percentage of the light signal so it can be examined. This is the purpose of the special cabinet referred to above: Circuits are connected into it, the light signal is split into two signals, one of which is diverted to the "secret room." The cabinet is totally unnecessary for the circuit to perform -- in fact it introduces problems since the signal level is reduced by the splitter -- its only purpose is to enable a third party to examine the data flowing between sender and recipient on the internet.

The above-referenced document includes a diagram (PDF 3) showing the splitting of the light signal, a portion of which is diverted to "SG3 Secure Room," i.e., the so-called "Study Group" spy room. Another page headlined "Cabinet Naming" (PDF 2) lists not only the "splitter" cabinet but also the equipment installed in the "SG3" room, including various Sun devices, and Juniper M40e and M160 "backbone" routers. PDF file 4 shows one of many tables detailing the connections between the "splitter" cabinet on the 7th floor (location 070177.04) and a cabinet in the "secret room" on the 6th floor (location 060903.01). Since the San Francisco "secret room" is numbered 3, the implication is that there are at least several more

in other cities (Seattle, San Jose, Los Angeles and San Diego are some of the rumored locations), which likely are spread across the United States.

One of the devices in the "Cabinet Naming" list is particularly revealing as to the purpose of the "secret room": a Narus STA 6400. Narus is a 7-year-old company which, because of its particular niche, appeals not only to businessmen (it is backed by AT&T, JP Morgan and Intel, among others) but also to police, military and intelligence officials. Last November 13-14, for instance, Narus was the "Lead Sponsor" for a technical conference held in McLean, Virginia, titled "Intelligence Support Systems for Lawful Interception and Internet Surveillance." Police officials, FBI and DEA agents, and major telecommunications companies eager to cash in on the "war on terror" had gathered in the hometown of the CIA to discuss their special problems. Among the attendees were AT&T, BellSouth, MCI, Sprint and Verizon. Narus founder, Dr. Ori Cohen, gave a keynote speech. So what does the Narus STA 6400 do?

"The (Narus) STA Platform consists of stand-alone traffic analyzers that collect network and customer usage information in real time directly from the message.... These analyzers sit on the message pipe into the ISP (internet service provider) cloud rather than tap into each router or ISP device" (*Telecommunications* magazine, April 2000). A Narus press release (1 Dec., 1999) also boasts that its Semantic Traffic Analysis (STA) technology "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) is the only technology that provides complete visibility for all internet applications."

To implement this scheme, WorldNet's high-speed data circuits already in service had to be rerouted to go through the special "splitter" cabinet. This was addressed in another document of 44 pages from AT&T Labs, titled "SIMS, Splitter Cut-In and Test Procedure," dated 01/13/03 (PDF 5-6). "SIMS" is an unexplained reference to the secret room. Part of this reads as follows:

> **"A WMS (work) Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document....**
> "This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits."

The NOC referred to is in Bridgeton, Missouri, and controls WorldNet operations. (As a sign that government spying goes hand-in-hand with union-busting, the entire (Communication Workers of America) Local 6377 which had jurisdiction over the Bridgeton NOC was wiped out in early 2002 when AT&T fired the union work force and later rehired them as nonunion "management" employees.) The cut-in work was performed in 2003, and since then new circuits are connected through the "splitter" cabinet.

Another "Cut-In and Test Procedure" document dated January 24, 2003, provides diagrams of how AT&T Core Network circuits were to be run through the "splitter" cabinet (PDF 7). One page lists the circuit IDs of key Peering Links which were "cut-in" in February 2003 (PDF 8), including ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, AboveNet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet and Mae West. By the way, Mae West is one of two key internet nodal points in the United States (the other, Mae East, is in Vienna, Virginia). It's not just WorldNet customers who are being spied on -- it's the entire internet.

The next logical question is, what central command is collecting the data sent by the various "secret rooms"? One can only make educated guesses, but perhaps the answer was inadvertently given in the DOD Inspector General's report (cited above):

> "For testing TIA capabilities, Darpa and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real-time feedback. The main node of TIA is located at INSCOM (in Fort Belvoir, Virginia)…."

Among the agencies participating or planning to participate in the INSCOM "testing" are the "National Security Agency, the Defense Intelligence Agency, the Central Intelligence Agency, the DOD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command and the Joint Warfare Analysis Center." There are also "discussions" going on to bring in "non-DOD federal agencies" such as the FBI.

This is the infrastructure for an Orwellian police state. It must be shut down!