Statement
—Mark Klein, April 6, 2006

My Background:

For 22 and ½ years I worked as an AT&T technician, first in New York and then in California.

What I Observed First-Hand:

In 2002, when I was working in an AT&T office in San Francisco, the site manager told me to expect a visit from a National Security Agency agent, who was to interview a management-level technician for a special job. The agent came, and by chance I met him and directed him to the appropriate people.

In January 2003, I, along with others, toured the AT&T central office on Folsom Street in San Francisco –actually three floors of an SBC building. There I saw a new room being built adjacent to the 4ESS switch room where the public's phone calls are routed. I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room. The regular technician workforce was not allowed in the room.

In October 2003, the company transferred me to the San Francisco building to oversee the WorldNet Internet room, which included large routers, racks of modems for customers' dial-in services, and other equipment. I was responsible for troubleshooting problems on the fiber optic circuits and installing new circuits.

While doing my job, I learned that fiber optic cables from the secret room were tapping into the Worldnet circuits by splitting off a portion of the light signal. I saw this in a design document available to me, entitled "Study Group 3, LGX/Splitter Wiring, San Francisco" dated December 10, 2002. I also saw design documents dated January 13, 2004 and January 24, 2003, which instructed technicians on connecting some of the already in-service circuits to the "splitter" cabinet, which diverts some of the light signal to the secret room. The circuits listed were the Peering Links, which connect WorldNet with other networks and hence the whole country, as well as the rest of the world.

One of the documents listed the equipment installed in the secret room, and this list included a Narus STA 6400, which is a "Semantic Traffic Analyzer". The Narus STA technology is known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets. The company's advertising boasts that its technology "captures comprehensive customer usage data...and transforms it into actionable information...[It] provides complete visibility for all Internet applications."

My job required me to connect new circuits to the “splitter” cabinet and get them up and running. While working on a particularly difficult one with a technician back East, I learned that other such “splitter” cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

What is the Significance and Why Is It Important to Bring These Facts to Light

Based on my understanding of the connections and equipment at issue, it appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the Internet— whether that be peoples’ email, web surfing, or any other data.

Given the public debate about the constitutionality of the Bush administration’s spying on US citizens without obtaining a FISA warrant, I think it is critical that this information be brought out into the open, and that the American people be told the truth about the extent of the administration's warrantless surveillance practices, particularly as it relates to the Internet.

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. 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.

Attorney contact information:

Miles Ehrlich
Ramsey & Ehrlich LLP