Statement of Telecommunications Expert Brian Reid

I am a telecommunications and data networking expert who has been involved in the development of several critical internet technologies. I was a professor of electrical engineering at Stanford University and of computer science at Carnegie Mellon University West.

Brian Reid is currently the Director of Engineering and Technical Operations at Internet Systems Consortium, a non-profit organization devoted to supporting a non-proprietary Internet.

I have carefully reviewed the AT&T authenticated documents and declaration provided by Mark Klein, and the public redacted version of the expert declaration of J. Scott Marcus, both filed in the Hepting v. AT&T litigation. Combining the information contained in those declarations and documents with my extensive knowledge of the international telecommunications infrastructure and the technology regularly used for lawful surveillance pursuant to warrants and court orders, I believe Mr. Klein's evidence is strongly supportive of widespread untargeted surveillance of ordinary people, both AT&T customers and others.

The AT&T Technological Setup

The AT&T documents describe a technological setup at the AT&T facility in San Francisco. This setup is particularly well-suited to wholesale, dragnet surveillance of all communications passing through that facility, whether international or domestic. These documents describe how the fiber optic cables were cut and splitters installed at the cut point.

Fiber optic splitters work just like ordinary TV splitters. One cable feeds in, and two cables feed out. Both cables carry a copy of absolutely everything that is sent, and if the second cable is connected to a monitoring station, that station sees all traffic going over the cable.

Mr. Klein stated that the second cable was routed into a room at the facility whose access was restricted to AT&T employees having clearances from the National Security Agency (NSA). The documents indicate that similar facilities were being installed in Seattle, San Jose, Los Angeles and San Diego. The documents also reference a somewhat similar facility in Atlanta.

This infrastructure is capable of monitoring all traffic passing through the AT&T facility (some of it not even from AT&T customers), whether voice or data or fax, international or domestic. The most likely use of this infrastructure is wholesale, untargeted surveillance of ordinary Americans at the behest of the NSA. NSA involvement undermines arguments that the facility is intended for use by AT&T in protecting its own network operations.

AT&T's Setup is Not Appropriate for Targeted or Merely International Surveillance.

This infrastructure is not limited to, nor would it be especially efficient for, targeted surveillance, or even untargeted surveillance aimed at communications where one of the ends is located outside the United States. It is also not reasonably aimed at supporting AT&T operations and security procedures. There are three main reasons:

- **Massive, "Real-Time" Surveillance Capability.** The technological infrastructure is far more powerful and expensive than that needed to do targeted surveillance or surveillance aimed only at international or one-end foreign communications. For example, it includes a NARUS 6400, a computer that can:
  - — Simultaneously analyze huge amounts of information based on rules provided by the machine operator.
  - — Analyze the content of messages and other information, not just headers or routing information.
  - — Conduct the analysis in "real time," rather than after a delay.
  - — Correlate information from multiple sources, multiple formats, over many protocols and through different periods of time in that analysis.
- **Capability to Secretly Move Huge Amounts of Data from the facility Elsewhere.** The documents describe a secret, private backbone network separate from the public network where normal AT&T customer traffic is carried transmitted. A separate backbone network would not be required for transmission of the smaller amounts of data captured via targeted surveillance. You don't need that magnitude of transport capacity if you are doing targeted surveillance.
- **Downtown San Francisco Location of the Equipment.** The San Francisco facility is not located near an entry/exit point for international communications that happen to be transmitted through the United States, either through undersea cable or via satellite. As a result, it would not be a sensible place to locate a facility aimed at simply monitoring traffic to or from foreign countries.

Contacts: Kevin Bankston of EFF at (415) 748-8126 or Adam Eisgrau (202) 215-6884