represented perhaps 20% of all Internet traffic in the United States: 20% * 50% = 10%.

126. It must be emphasized that this estimate does not mean that traffic was intercepted merely for 10% of AT&T customers; rather, it means more than half of all Internet traffic was likely intercepted (at least, at a physical level) for *all* AT&T customers. Moreover, it means that about 10% of all U.S. Internet traffic was physically intercepted for *all* U.S. Internet users, including non-AT&T customers.

127. The estimate of 10% also assumes that only AT&T implemented [redacted] Configurations or their equivalent, since the AT&T deployments are the only ones that are demonstrated by the documents that I was asked to review. If other carriers had deployed configurations similar to the [redacted] Configurations – feeding in, for example, to the same centralized correlation and analysis center or centers – then the percentage would of course be higher.

ALTERNATIVE REASONS WHY AT&T MIGHT HAVE DEPLOYED THE [redacted] CONFIGURATIONS

128. The Klein Declaration states that the [redacted] area was a Secure Room, and that only NSA-cleared personnel were permitted to enter. In this section, I consider whether it is credible that the [redacted] Room described in the AT&T documents was in fact a secure facility funded by the government. I conclude that it is highly probable.

129. Given the size and the scope of the build-out, and given AT&T's financial difficulties at the time, I consider it highly unlikely that AT&T undertook the development on its own. There is no apparent commercial justification.

130. First, the [redacted] Configuration is not useful for carrying Internet traffic. No provider wants to make duplicate copies of the same packets – it costs money to transport the packets, and they provide no corresponding benefits to the user.

131. Second, AT&T might have deployed the [redacted] configurations in order to sell security services to their customers. AT&T does in fact offer a service called Internet Protect to its Internet access customers, and the service appears to be based on the [redacted] offering. Indeed, this is the

rationale indicated on the [redacted] website.[47] Indications are that the service has not been nearly profitable enough to justify the [redacted] expenditure;[48] still it is possible that AT&T might have overestimated demand.

132. This explanation also falls short. The [redacted] Configurations were deployed beginning in early 2003, meaning that planning was probably under way six to twelve months earlier, given AT&T process. Internet Protect was not announced until March, 2004.[49] Aside from that, AT&T officials themselves characterized aspects of Internet Protect as something that they had already deployed for other purposes, and only belatedly realized might benefit their customers.[50] All indications are the Internet Protect was an attempt to extract commercial value from a deployment already made – or more likely, from a new deployment using the same technology as the [redacted] Configuration – rather than having been the original rationale for the deployment.

133. Third, it is possible that AT&T might have deployed the [redacted] configuration in order to meet obligations for lawful intercept. The [redacted] system can be used for this purpose; however, it is not credible that this was the rationale for the deployment. Far simpler and far less expensive solutions could have met all the limited CALEA requirements that were in force at the time of

---

[47] [redacted]

[48] "AT&T has packaged that help in a service it calls AT&T Internet Protect, but so far few large agencies have signed up. Buying managed security services from AT&T and other carriers might take some time to catch on, if it ever does, said Timothy McKnight, chief information security officer at Northrop Grumman. "There's a lot of value there, and I agree they should bring it to the table," he said." *See* http://www.fcw.com/article90916-09-26-05-Print (Exhibit V).

[49] http://www.att.com/news/2004/03/22-12972 (Exhibit W).

[50] "Project Gemini, for which development began nearly a year ago, sprang from AT&T's belief that it could better manage customers' security by having the defenses on the company's IP backbone network rather than simply administering security devices on the customers' premises. . . . In addition to the network-based services, AT&T is also working on a security event management system called Aurora that it plans to sell as a software solution. The system relies on the company's Daytona database and is designed to do more than simple event correlation and normalization. . . . AT&T has been using Aurora internally for approximately 18 months, Amoroso said, and only started selling the event management system on a limited basis recently after a customer saw the system and asked for it." Eweek, "Security on the Wire", November 22, 2004, at http://www.eweek.com/print_article2/0,1217,a=139716,00.asp (Exhibit X).

deployment.[51] Workstation solutions, like those in use at Genuity at the time, would have been sufficient to meet legal requirements. The FBI's Carnivore provides a good example of a far more cost-effective solution.[52] (The [redacted] Configurations provide a much more capable solution, but in my judgment the company would never have made the substantial incremental investment unless other factors were in play.)

134. Fourth, AT&T might have deployed the system in order to enhance its internal security. This is a somewhat more plausible explanation, but I believe on examination it is far from adequate to explain the investment. It is true that this configuration can be used to protect against distributed denial of service (DDoS) attacks and a number of additional security challenges, but the aggregate benefits do not approach the level of investment made.

135. I considered several alternative hypotheses, including (1) enhanced security for U.S. government customers of AT&T WorldNet; (2) data mining of AT&T customers; and (3) support for sophisticated, possibly application-specific billing and accounting measurements. None of these possibilities would appear to account for the investment that AT&T apparently made in the [redacted] Configurations.

136. In sum, I can think of no business rationale in terms of AT&T's own business needs that would likely have justified an investment of this magnitude, nor any combination of rationales.

137. With that in mind, I consider it highly probable that this deployment was externally funded, and I consider the U.S. Government to be the most obvious funding source.

138. The presence of the [redacted] is consistent with this assessment. It is far easier to reconcile the presence of a private network with a covert project than it is to explain its presence in the context of normal AT&T operations. AT&T would most likely have used the Common Backbone for routine internal management or operational needs.

139. The [redacted] Configuration is, at a technical level, an excellent fit with the requirements

---

[51] The FCC did not impose CALEA requirements on broadband or on Voice over IP (VoIP) until 2005.

[52] Marcus Thomas of the FBI described Carnivore to the North American Network Operators' Group (NANOG) in 2000. The video presentation is available at http://www.nanog.org/mtg-0010/carnivore.html; see also http://videolab.uoregon.edu/nanog/carnivore/.

of a massive, distributed surveillance project. In my opinion, and based on my experience, no other intended purpose explains as well the constellation of design choices that were made.

AT&T'S FINANCIAL CONDITION IN 2003

140. I consider it unlikely that AT&T would have made discretionary investments of this magnitude on its own initiative (with no apparent prospect of return) under any circumstances, but I consider it particularly implausible given the condition of the company in 2003.

141. Lehman Brothers issued investment guidance on AT&T on January 24, 2003, the same day on which Klein Exhibit B was issued. This guidance provides useful historic perspective on the financial state of AT&T as viewed by a knowledgeable and informed observer at the time.[53]

142. In the January 2003 assessment, Lehman Brothers lowered their target stock price from $25 to $20, and recommended that investors underweight AT&T in their portfolios. This reflects a dramatic, precipitous decline. In May 2000, their target had been $400. In January 2001, it was $200. As recently as October 2002, it had been $70.

143. The Lehman Brothers analysis shows a rapid 20% decline in revenues on the part of AT&T Consumer Services, and they predicted a 25-30% decline for 2003. 100% RBOC entry into long distance was already anticipated, as was the FCC's imminent elimination of UNE-P.[54] Lehman Brothers therefore anticipated that AT&T would be forced to exit the Consumer Services business within the year.

144. The profitability of AT&T Business Services was also under pressure – 40% of its revenues came from wholesale long distance voice, where margins were already thin and continuing to decline.

145. In short, most of the financial pressures that ultimately drove AT&T to be acquired by SBC were already evident at the time that these investments were made.

---

[53] A copy of the Lehman Brothers analysis is attached as Exhibit Y to my declaration.

[54] Regional Bell Operating Company (RBOC) entry into long distance would represent increased competition for AT&T's consumer long distance business; the FCC's phasing out of the obligation on RBOCs to provide the Unbundled Network Element Platform (UNE-P) would eliminate AT&T's ability to profitability compete with the RBOCs in offering local services. The combined effect would be to eliminate AT&T's ability to compete with the RBOCs for consumer customers seeking flat rate plans comprising both local service and long distance.

146. Given that there is no apparent revenue justification for the deployment of the [redacted] Configurations, I would have expected AT&T to defer discretionary investments at that time. I therefore infer that the deployment was with high probability either externally funded or externally subsidized.

147. This assessment supports the plausibility of the Klein Declaration as regards a government role in the [redacted] Configurations.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed March 29, 2006 at Bonn, Germany.

J. Scott Marcus

J. SCOTT MARCUS

CERTIFICATE OF SERVICE

I hereby certify that on June 22, 2006, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the following non-CM/ECF participants:

David W. Carpenter
Sidley Austin Brown & Wood LLP
Bank One Plaza
10 South Dearborn Street
Chicago, IL 60600

David L. Lawson
Sidley Austin Brown & Wood
1501 K Street, N.W.
Washington, D.C. 20005

Susan Freiwald
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117

Eric Schneider
1730 South Federal Hwy. #104
Delray Beach, FL 33483

By /s/
Cindy A. Cohn, Esq. (SBN.145997)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
cindy@eff.org