Our next largest peering partners changed somewhat over time, but typically included Qwest, Level3, Verio and Cable and Wireless. Public peering points such as MAE-West represented a small and steadily diminishing percentage of our peering traffic. AT&T had a larger customer base than Genuity, but one might expect the relative proportions to be generally similar, with the obvious exception of AT&T's traffic to itself. The relative sizes of peering circuits on the last page of Klein Exhibit B is not inconsistent with this assumption. Genuity had peering arrangements with 50 to 60 networks, but many of them exchanged relatively little traffic with us. All of our significant peering partners at that time appear on the list on the last page of Klein Exhibit B.

106. I therefore infer either that: (1) all of the networks with which AT&T peered in [redacted] had their traffic intercepted, or else (2) any AT&T peering partners whose traffic was not intercepted most likely were small networks that exchanged very little traffic with AT&T.

107. The traffic intercepted at the [redacted] facility probably represented a substantial fraction of AT&T's total national peering traffic, but the percentage is unimportant for this analysis.

108. In my judgment, significant traffic to and from the plaintiffs (especially those in the [redacted]) would have been available for interception by the [redacted] Configuration, even if [redacted] had only been implemented in [redacted]. As of the end of 2002, AT&T most likely had West Coast peering to other major backbones at three major locations at most [redacted]. As noted above, the major peers were present at [redacted], probably representing all or substantially all of AT&T's peering traffic in the [redacted]. Off net traffic *from* the plaintiffs would have been handed off to peers at the first available opportunity (a process referred to as "shortest exit" or "hot potato" routing), and thus would with high probability have been handed off through the [redacted] facility. Off net traffic *to* the plaintiffs could have been presented to AT&T using peering connections at any of perhaps eight different cities, so a significant fraction of the total would have passed through [redacted], but not all.

109. I conclude that the designers of the [redacted] Configuration made no attempt, in terms of the location or position of the fiber split, to exclude data sources comprised primarily of domestic

data. A fiber splitter, in its nature, is not a selective device – all the traffic on the split circuit was diverted or copied. In my experience, backbone ISPs typically provide a single peering circuit for peering traffic at a given location – they do not provide separate circuits for domestic peering traffic as distinct from international peering traffic. Most of the backbone ISPs that appear in Klein Exhibit B had substantial U.S.-based business, and probably carried significantly more domestic traffic than international.

110. Once the data has been diverted, there is nothing in the data that reliably and unambiguously distinguishes whether the source or destination is domestic or foreign. AT&T would know with near certainty the location of the side of the communication that originated or terminated with its own customer (nearly always domestic in this case), but it would be limited in its ability to determine the location of the other side of the communication. This is because *IP addresses, unlike phone numbers, are not associated with a user's physical location.*

111. There are software programs that attempt to infer physical location from an IP address (a process referred to as *geolocation*). Geolocation is an inherently error-prone process, but some vendors claim, rightly or wrongly, an accuracy of 95% or better. The question of correctness must, however, be considered in the context of the accuracy required. When the FCC considered the geolocation problem in terms of its impact on VoIP users seeking access to emergency services, we were concerned with the possibility of identifying the user's location with sufficient accuracy to enable a policeman or ambulance driver to physically find the caller. In this case, however, it is only necessary to determine whether an IP address is inside the United States. Assuming *arguendo* that the data intercepted by the [redacted] Configurations was indeed captured for purposes of surveillance, it is possible that purely domestic communications could have been excluded with a reasonably high success rate. It is nonetheless safe to say that, even had there been a serious attempt to exclude purely domestic communications, some purely domestic communications would have slipped through the filter and been analyzed anyway.

112. The documents provide no basis on which to determine whether geolocation was attempted. Given (under the foregoing assumptions) that all of the international data was going to be evaluated by a sophisticated high speed inference engine (the [redacted] system) in any case, the

simpler, cheaper and more natural engineering approach would be to use the Narus system to evaluate all of the data, both domestic and foreign, and to leave it to the inference engine to determine which data was interesting.

NUMBER OF LOCATIONS

113. The Klein Declaration states that [redacted] were being installed in other cities, including [redacted]. Unlike most statements in the Klein Declaration, this one is not based on his first hand knowledge. It is therefore appropriate to consider first, whether the assertion is plausible, and second, how large a total deployment it implies.

114. Based on my assessment of the AT&T documents, I consider the assertion to be plausible, and to be consistent with an overall national AT&T deployment to from 15 to 20 sites, possibly more.

115. Klein Exhibit B talks about general AT&T naming conventions, and says: [redacted][43] This emphasis on a standardized, cookie-cutter approach is consistent with AT&T standard practice, but also implies a planned deployment to multiple sites, surely more than two or three.

116. All of these documents need to be understood in terms of AT&T practices and priorities. AT&T is used to operating networks on a large scale, with centralized highly skilled engineers and with a field force at a lower skill level. This implies the need for a highly structured approach to describing the work to be done, and precise, meticulous instructions. AT&T had clearly gone to great lengths to standardize the design of their CBB locations as much as possible; nonetheless, for a variety of reasons, the locations were not identical. The directions therefore try to strike a balance between first describing the general case for all locations, and then providing site-specific directions that apply the general directions to the circumstances of a particular CBB

[42] As previously note, the [redacted] refers to an equipment rack. I infer that the [redacted] refers to an AT&T convention that assigns a unique and unambiguous identifier that is suitable for site-specific work.

[43] Klein Exh. B, p. 4.

location.

117. Page 5 of Klein Exhibit A discusses the various racks [redacted] involved, and says of the [redacted] If the planned deployment were for only two or three sites, the universality of [redacted] would not have been in doubt. This again hints at a large enough deployment that it was inconvenient to check all of the necessary background plans.

118. On the same page, Klein Exhibit A refers to [redacted] different rack arrangements that could be present at any given site. On site staff would only need to familiarize themselves with the single configuration present at their site. This implies an absolute minimum of [redacted] sites; however, I consider it unlikely that they would go to this much trouble in crafting such general language if that were the case. Klein Exhibit A specifically states on page 17: "[redacted]" The absence of similar statements for Arrangements 1, 2 and 3 implies that there are [redacted] or more instances of each of those rack arrangements. Again, this is consistent with a deployment to 15 to 20 [redacted] Room sites if not more.

TRAFFIC CAPTURED BY MULTIPLE [redacted] ROOMS

119. I have already explained that an enormous amount of Internet traffic is likely to have been captured by the devices in the [redacted] Room in [redacted]. I now briefly consider the volume of Internet traffic that would be captured if there were multiple [redacted] rooms.

120. Assuming that AT&T deployed [redacted] Configurations to as many locations as appears to have been the case, it is highly probable that all or substantially all of AT&T's traffic to and from other Internet providers anywhere in the United States was diverted.

121. If Internet backbone A were carrying x% of all Internet traffic, and if its customers were no more likely to interact with other A customers than with any other provider's customers, then one would expect x% of backbone A's traffic would stay on net and that 100% - x% of A's traffic would go off net (to other providers).[44] In practice, a somewhat higher fraction usually stays

[44] This is the same methodology used in my paper with Laffont, Tirole and Rey. Exhibit D, pp. 373-74.

on net for a variety of reasons.

122. Based on my knowledge of Genuity's traffic flows in 2001, and based also on AT&T's claims that it had grown to become the largest Internet backbone as of late 2002,[45] I would estimate that AT&T was carrying something like 20% of U.S. Internet backbone traffic in late 2002. This estimate reflects the assumption that Genuity's traffic pattern was fairly typical of that of other providers. If AT&T was carrying 20% of all U.S. Internet traffic, and if AT&T customers were no more likely to communicate with other AT&T customers than with customers of any other ISP, then one would expect that about 100% - 20% = 80% of AT&T customer traffic would be destined off net. Given that some traffic tends to stay on net for other reasons – for example, traffic between multiple sites of the same corporation, all of which use AT&T as a provider – I would estimate that somewhere between 60% and 80% of AT&T's customer traffic was going off net.

123. This implies that nearly all of AT&T's international traffic was diverted, with the apparent exception of traffic from an AT&T customer to an overseas AT&T customer.[46]

124. *It also implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted, representing all or substantially all of the AT&T traffic handed off to other providers.* This proportion is somewhat less than the 60%–80% estimated above, because it excludes the international traffic.

125. The volume of *purely domestic* communications available for inspection by the [redacted] Configurations thus appears to be very substantial. *I estimate that a fully deployed set of Configurations would have captured something in the neighborhood of 10% of all purely domestic Internet communications in the United States.* This estimate follows from my previous estimates. The [redacted] Configurations intercepted more than 50% of all AT&T domestic traffic, which

[45] See remarks of Hossein Eslambolchi, AT&T labs president and chief technology officer, quoted in BroadbandWeek Direct at http://www.broadbandweek.com/newsdirect/0208/direct020802.htm, August 2, 2002 ("AT&T has been steadily growing its backbone traffic and now expects to surpass WorldCom as the sector leader in a few months …") (Exhibit T).

[46] To the extent that AT&T has overseas customers, their traffic to other AT&T customers would not appear as peering traffic and therefore would not be intercepted by the [redacted] Configurations as described in the AT&T documents.