

1 ELECTRONIC FRONTIER FOUNDATION
 2 CINDY COHN (145997)
 3 cindy@eff.org
 4 LEE TIEN (148216)
 5 tien@eff.org
 6 KURT OPSAHL (191303)
 7 kurt@eff.org
 8 KEVIN S. BANKSTON (217026)
 9 bankston@eff.org
 10 CORYNNE MCSHERRY (221504)
 11 corynne@eff.org
 12 JAMES S. TYRE (083117)
 13 jstyre@eff.org
 14 454 Shotwell Street
 15 San Francisco, CA 94110
 16 Telephone: 415/436-9333
 17 415/436-9993 (fax)

10 TRABER & VOORHEES
 11 BERT VOORHEES (137623)
 12 bv@tvlegal.com
 13 THERESA M. TRABER (116305)
 14 tmt@tvlegal.com
 15 128 North Fair Oaks Avenue, Suite 204
 16 Pasadena, CA 91103
 17 Telephone: 626/585-9611
 18 626/ 577-7079 (fax)

LAW OFFICE OF RICHARD R. WIEBE
 RICHARD R. WIEBE (121156)
 wiebe@pacbell.net
 425 California Street, Suite 2025
 San Francisco, CA 94104
 Telephone: 415/433-3200
 415/433-6382 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

18 UNITED STATES DISTRICT COURT
 19 FOR THE NORTHERN DISTRICT OF CALIFORNIA

20 TASH HEPTING, GREGORY HICKS,
 21 CAROLYN JEWEL and ERIK KNUTZEN, on
 22 Behalf of Themselves and All Others Similarly
 23 Situated,,

Plaintiffs,

v.

25 AT&T CORP., et al.,

26 Defendants.

No. C-06-0672-VRW

CLASS ACTION

**DECLARATION OF J. SCOTT MARCUS
 IN SUPPORT OF PLAINTIFFS'
 MOTION FOR PRELIMINARY
 INJUNCTION**

Date: June 8, 2006
 Courtroom: 6, 17th Floor
 Judge: Hon. Vaughn Walker

REDACTED PUBLIC VERSION

LIST OF EXHIBITS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- A Curriculum vitae of J. Scott Marcus
- B Eric Lichtblau and James Risen, Spy Agency Mined Vast Data Trove, Officials Report, The New York Times, Dec. 24, 2005
- C Barton Gellman, Dafna Linzer and Carol D. Leonnig, Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared, Washington Post, Feb. 5, 2006
- D Marcus et al, "Internet interconnection and the off-net-cost pricing principle"
- E Marcus, "Call Termination Fees: The U.S. in global perspective"
- F Marcus, "What Rules for IP-enabled NGNs?"
- G "Evolving Core Capabilities of the Internet"
- H <http://en.wikipedia.org/wiki/Modulation>
- I <http://en.wikipedia.org/wiki/Attenuation>
- J <http://en.wikipedia.org/wiki/Decibel>
- K ADC brochure (Value-Added Module System: LGX Compatible)
- L [REDACTED]
- M [REDACTED]
- N [REDACTED]
- O [REDACTED]
- P [REDACTED]
- Q In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, FCC WC Docket 02-361, Petition of AT&T
- R Report of the NRIC V Interoperability Focus Group, "Service Provider Interconnection for Internet Protocol Best Effort Service"
- S Ch. 14, Marcus, Designing Wide Area Networks and Internetworks: A Practical Guide (1999)
- T <http://www.broadbandweek.com/newsdirect/0208/direct020802.htm>, August 2, 2002
- U [REDACTED]
- V <http://www.few.com/article90916-09-26-05-Print>
- W <http://www.att.com/news/2004/03/22-12972>

1 X http://www.eweek.com/print_article2/0,1217,a=139716,00.asp

2 Y Lehman Brothers analysis of AT&T (Jan. 24, 2003)

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 I, J. Scott Marcus, declare under the penalty of perjury that the following is true and
2 correct:

3 1. The Electronic Frontier Foundation (EFF) has asked me to render an expert opinion¹
4 on the implications of a declaration by Mark Klein ("Klein Declaration"), and on a series of
5 documents alleged to have been generated by AT&T (Exhibits A, B and C to the Klein
6 Declaration) ("Klein Exhibits"), in conjunction with Plaintiffs' Motion for a Preliminary Injunction.

7 2. I am strongly of the opinion that the Klein Exhibits are authentic, and I find Mr.
8 Klein's declaration to be fully consistent with the documents and entirely plausible.

9 3. The EFF specifically requested that I assess whether the program described in the
10 Klein Declaration and Klein Exhibits is consistent with media reports about a program authorized
11 by the President of the United States, under which the National Security Agency ("NSA") engages
12 in warrantless surveillance of communications of people inside the United States ("the Program").

13 4. I was asked to review the following two news articles: Eric Lichtblau and James
14 Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, The New York Times, Dec. 24, 2005
15 (attached as Exhibit B), and Barton Gellman, Dafna Linzer and Carol D. Leonnig, *Surveillance Net*
16 *Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are*
17 *Later Cleared*, Washington Post, Feb. 5, 2006 at A01 (attached as Exhibit C).

18 5. I was asked to focus on the following claims in these two news articles, with respect
19 to AT&T Corp.: that major U.S. telecommunications companies are assisting the government in
20 carrying out the Program; that these companies have given the government direct access to
21 telecommunications facilities physically located on U.S. soil; that by virtue of this access, the
22 government can now monitor both domestic and international communications of persons in the
23 United States; and that surveillance under the Program is conducted in several stages, with the
24 early stages being computer-controlled collection and analysis of communications and the last
25 stage being actual human scrutiny.

26 6. In the sections that follow, I present my qualifications, and provide an overview of
27

28 ¹ Attached hereto as Exhibit A is my curriculum vitae.

1 the implications of the Klein Declaration and Klein Exhibits. I present my conclusions in regard to
2 the scope of the program, and the volume of data that was captured. I also explain why I find
3 credible Mr. Klein's allegation that the room described was a secure facility, intended to be used
4 for purposes of surveillance on a very substantial scale.

5 QUALIFICATIONS

6 7. For more than 30 years, I have worked in a wide range of positions involving
7 computers, data communications, economics, and public policy. This declaration draws on my
8 experience in several of these positions, and in several different academic disciplines.

9 8. From March 1990 to July 2001, I held a series of responsible positions with Bolt,
10 Beranek and Newman (which was renamed BBN Corp.) and with its successor companies, GTE
11 Internetworking and Genuity, culminating in my work as Chief Technology Officer (CTO) of
12 Genuity.

13 9. BBN Corp. was acquired by GTE Corp. in 1997. The portion of BBN that
14 functioned as an Internet Service Provider (ISP)² became GTE Internetworking, a wholly owned
15 subsidiary of GTE.

16 10. In 2000, at the time of the Bell Atlantic – GTE merger (which formed Verizon),
17 GTE Internetworking was spun out into an independent company in order to satisfy regulatory
18 obligations relevant to the merger. The independent firm was called Genuity.

19 11. My primary engineering competence is as a designer of large scale IP-based³ data
20 networks.

21 12. Immediately following BBN's acquisition by GTE, I headed the team of systems
22 architects and network engineers who developed the overall architectural design for GTE
23 Internetworking's new data network. The team, comprising of as many as 50 senior engineers at
24 various times, translated general business and marketing requirements into a comprehensive set of

25
26 ² An *Internet Service Provider (ISP)* is an organization that enables other organizations to
27 connect to the global Internet. ISPs often provide additional supporting services to enable
28 electronic mail (e-mail) and to permit domain names (such as www.fcc.gov) to be recognized.

³ All Internet traffic is *IP-based*, i.e. based on the Internet Protocol. I expand on this discussion in
the section in which I discuss "Traffic captured".

1 high level engineering designs. This was a project of substantial scope and scale. The new network
2 transformed 13,000 miles of dark fiber⁴ into a single integrated network providing nationwide (and
3 ultimately global) high speed Internet access services, and support for consumer Internet access via
4 broadband and dial-up, and high speed data services for large enterprises. In terms both of scope
5 and of technology, this network was at the state of the art of the day. The network was viewed as a
6 technical and economic success, and became in short order one of the largest Internet backbone
7 networks in the world – in terms of traffic carried, it could be viewed as the fourth largest Internet
8 *backbone*⁵ in the world for much of the time that I was there.

9 13. I have some experience with AT&T's network at its inception. When AT&T
10 initially entered the Internet business in 1995, they contracted with my firm, BBN, to provide the
11 underlying service. In effect, they "private labeled" a BBN service. They provided connections to
12 their customers over dedicated circuits, which were cross-connected to BBN's Internet network.
13 The customer perceived an AT&T-branded service, but BBN provided the actual ISP services. I
14 was BBN's lead technical person for this endeavor.

15 14. BBN and AT&T conducted exploratory, but ultimately unsuccessful, discussions
16 about building an Internet backbone together. AT&T ultimately decided to implement their own
17 Internet backbone network (the Common Backbone [CBB]),⁶ which is the same name used in these
18 documents), and thus to assume the ISP functions that had previously been provided by BBN. The
19 initial design of the CBB reflected AT&T's experience in working with BBN.

20 15. In addition to the GTE Internetworking's own Internet backbone, and the work with
21 AT&T, I designed a number of networks for commercial and government customers. I did the
22 initial design work and cost analysis for a very large dial-up network for America Online in 1995.

23 _____
24 ⁴ Fiber optics are discussed later in this declaration. Dark fiber is fiber optic cable that is not
yet carrying traffic.

25 ⁵ The term *backbone* is widely used in the industry, but not precisely defined. An Internet
26 backbone can be thought of as a large ISP, many of whose customers may themselves be smaller
ISPs. There is no single network that is *the Internet*; rather, the Internet backbones collectively
27 form the core of the global Internet. The term backbone is also sometimes used to denote any large
IP-based network, whether used to provide IP-based services to the public or not.

28 ⁶ The AT&T Common Backbone, like backbones generally, is a large IP-based network. The CBB
is used for the transmission of interstate or foreign communications.

1 This network ultimately carried as much as 40% of America Online's dial-up traffic.

2 16. My experience as CTO at GTE Internetworking provides useful insights not only in
3 network design, but also into operational procedures in a large Internet backbone operator
4 associated with a large traditional telecommunications carrier. BBN's joint project with AT&T
5 required me to work closely with AT&T's engineers as they deployed the service. In addition,
6 much of BBN's Internet equipment was physically deployed into points of presence owned and
7 operated by WorldCom and by MCI, which required that I be able to coordinate with their staffs as
8 well. These insights into carrier operations enable me to assess the AT&T documents.

9 17. Many of my other duties at BBN, GTE Internetworking and Genuity are relevant to
10 this declaration.

11 18. I created a network design and capacity planning function within BBN, and ran the
12 function for several years. In the context of an ISP, capacity planning is the process whereby the
13 ISP measures and interprets current service demands on the network, projects future demands
14 (considering both current and projected future service offerings), and plans for necessary network
15 enhancements to meet those demands. Capacity planning required constant interaction with the
16 company's financial planners, as well as marketing and engineering. It also required an in-depth
17 understanding of traffic flows within and between Internet providers. After the merger with GTE, I
18 received a GTE Chairman's Leadership Award for that work.

19 19. I am the author of a textbook on data network design: *Designing Wide Area*
20 *Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999. The book largely reflects
21 my experience with capacity planning and network design in the large at BBN, GTE
22 Internetworking and Genuity.

23 20. I held a number of sales and marketing positions at BBN, and in those roles (and
24 also subsequently as Genuity's CTO) frequently participated in the assessment of the costs and the
25 potential revenues associated with new services.

26 21. Many of my outside consulting assignments at BBN involved elements of data
27 security and network security. Later, as CTO, the company's senior security expert was a direct
28 report. I thus had a general oversight role with respect to the company's performance of lawful

1 intercept.

2 22. As CTO, I also had primary responsibility for the company's strategic approach to
3 peering⁷ with other Internet Service Providers (including AT&T). I personally chaired the firm's
4 peering policy council, where the company's various stakeholders (engineering, financial and
5 marketing) established strategic direction in regard to peering.

6 23. I supported GTE's General Counsel in raising concerns about the MCI-WorldCom
7 merger (1998) and the proposed MCI-Sprint merger (2000), arguing that the network externality
8 effects resulting from the mergers would make anticompetitive practices as regards Internet
9 backbone peering both feasible and profitable. These arguments hinged to a substantial degree on
10 my ability to estimate peering traffic flows between the major Internet backbones in both real and
11 hypothetical circumstances. This activity drew heavily on my experience with the measurement
12 and analysis of traffic.

13 24. From July 2001 to July 2005, I was the Senior Advisor for Internet Technology at
14 the Federal Communications Commission (FCC). In this role, I served as the FCC's leading
15 technical expert on the Internet, and provided advice to the Chairman's office and to other senior
16 managers as regards technology and policy issues.

17 25. I participated in numerous proceedings during my time at the FCC, including
18 several that dealt generally with broadband and with Voice over IP (VoIP).⁸

19 26. I was a member of the FCC's Homeland Security Policy Council, with significant
20 responsibilities as regards cybersecurity and infrastructure security. I held a top secret clearance. I
21 frequently spoke on the FCC's behalf on lawful intercept (CALEA)⁹ in connection with IP-based
22 services. I was an active and significant participant in the FCC's proceedings related to CALEA in
23

24 ⁷ *Peering* is the process whereby Internet providers interchange traffic destined for their
25 respective customers, and for customers of their customers. A more extensive definition appears
26 later in this Declaration, under "Traffic Captured."

26 ⁸ *IP* is the Internet Protocol. All Internet data is IP-based. *Voice over IP* refers to the
27 transmission of voice over IP-based networks – either private networks or the "public" Internet.

27 ⁹ Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-
28 414, 108 Stat. 4279. CALEA is the statute that requires carriers to proactively instrument their
networks in order to support law enforcement needs. The FCC has a role in its implementation.


1 connection with Voice over IP (VoIP) and with broadband.

2 27. From July 2005 to the present, I have been a Senior Consultant for the WIK, located
3 in Bad Honnef, Germany. The WIK is a leading German research institute specializing in the
4 economics of electronic communications, and the regulatory implications that flow from those
5 economics. Much of my current work applies economic reasoning to policy problems in electronic
6 communications.

7 28. I am a Senior Member of the Institute of Electrical and Electronics Engineers
8 (IEEE), and have held several senior volunteer positions within the IEEE. I am currently co-editor
9 for public policy and regulatory matters for *IEEE Communications Magazine*. I have also served as
10 a trustee of the American Registry of Internet Numbers (ARIN).

11 29. I do not consider myself an economist, but I have a good working knowledge of
12 economics as it applies to the aspects of telecommunications that I deal with. Several of my
13 professional papers over the past few years are economics papers, and a number of them have been
14 cited by recognized economists.¹⁰ Other recent papers apply economic reasoning to problems in the
15 regulation of electronic communications.¹¹

16 **BACKGROUND – DOCUMENTS REVIEWED**

17 30. In forming my expert opinions in this Declaration, I reviewed the following
18 documents: the Klein Declaration; 

19
20 ¹⁰ See, for instance, my paper with Jean-Jacques Laffont, Patrick Rey, and Jean Tirole, IDE-I,
21 Toulouse, "Internet interconnection and the off-net-cost pricing principle," *RAND Journal of*
22 *Economics*, Vol. 34, No. 2, Summer 2003, available at
23 <http://www.rje.org/abstracts/abstracts/2003/rje.sum03.Laffont.pdf> (Exhibit D). An earlier version
24 of the paper appeared as "Internet Peering," *American Economics Review*, Volume 91, Number 2,
25 May 2001. See also "Call Termination Fees: The U.S. in global perspective," presented at the 4th
26 ZEW Conference on the Economics of Information and Communication Technologies, Mannheim,
27 Germany, July 2004, available at: [ftp://ftp.zew.de/pub/zew-](ftp://ftp.zew.de/pub/zew-docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf)
28 [docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf](ftp://ftp.zew.de/pub/zew-docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf) (Exhibit E). Another paper that deals
primarily with economics has been commissioned by the International Telecommunications Union
(ITU-T) for presentation at their ITU New Initiatives Workshop on "What Rules for IP-enabled
NGNs?," March 23-24, 2006: "Interconnection in an NGN environment," available at
<http://www.itu.int/osg/spu/ngn/documents/Papers/Marcus-060323-Fin-v2.1.pdf> (Exhibit F).

¹¹ See, for instance, "Evolving Core Capabilities of the Internet," *Journal on*
Telecommunications and High Technology Law, 2004 (Exhibit G).

1 (Klein Decl. Exh. A); [REDACTED]

2 [REDACTED] (Klein Decl. Exh. B); and [REDACTED]

3 [REDACTED] (Klein Decl. Exh. C).

4 31. I have also reviewed publicly available data on the Internet – wherever I have relied
5 on such data, I have so indicated in the text.

6 32. The Klein Exhibits use terms such as [REDACTED] equipment” and [REDACTED] room.” I believe
7 [REDACTED] to be an acronym for [REDACTED], which is used consistently to describe the project.
8 Consistent with this terminology, I will refer to the [REDACTED] Configuration throughout this declaration.

9 33. I interpret [REDACTED] as a reference to the [REDACTED]. These documents
10 represent directions to technicians who must “cut” the new facilities into the network, *i.e.* install
11 them with as little impact as possible on AT&T’s ongoing network operations.

12 34. Based on my experience in working with AT&T, I consider the documents to be
13 written with the meticulous attention to detail that is typical of AT&T operations. Highly skilled
14 central engineering staff provided unambiguous and highly detailed directions in order to enable
15 implementation by multiple on site field crews at a lower skill level. Any operations that could be
16 done in advance were dealt with prior to the cut. The cut was designed to be as fast and as painless
17 as possible, so as to minimize the risk of network disruption. The cut was to take place during the
18 maintenance window (presumably during the early morning hours, *e.g.* 2:00 AM) so as to further
19 minimize possible disruption.¹²

20 35. It is clear that these plans relate to real deployments, and not just to a theoretical or
21 hypothetical exercise. The last page of Klein Exhibit B makes clear that the [REDACTED]
22 deployment was already in full swing when the document was published on [REDACTED]. Of
23 [REDACTED] large [REDACTED] circuits that were to be diverted, (1) circuit engineering was complete for
24 [REDACTED], (2) actual change orders had already been issued for [REDACTED], and were scheduled to be issued
25 for [REDACTED] more within the subsequent week (*i.e.* by [REDACTED]), and (3) request dates had been
26 established for the completion of the remaining circuit engineering, for [REDACTED] pre-test and for
27

28 ¹² See Klein Exh. A, page 4.

1 putting the [REDACTED] into the circuits, all in [REDACTED] and [REDACTED].

2 36. Klein Exhibit B and Klein Exhibit C are specific to AT&T's [REDACTED] facility,
3 but Klein Exhibit A is generic – it is relevant to all sites where this cut was to take place.

4 **OVERVIEW AND SUMMARY OF PRINCIPAL OPINIONS**

5 37. My expert assessment is based on the Klein Declaration, the AT&T documents
6 collectively designated as the Klein Exhibits, my extensive and varied experience in the industry,
7 and various publicly available documents. Where I have relied on such documents, I have so
8 indicated in the text.

9 38. Based on these documents, other publicly available documents, and my general
10 knowledge of the industry, I conclude that AT&T has constructed an extensive – and expensive –
11 collection of infrastructure that collectively has all the capability necessary to conduct large scale
12 covert gathering of IP-based communications information, *not only for communications to*
13 *overseas locations, but for purely domestic communications as well.*¹³

14 39. In terms of the media claims I was asked to evaluate with respect to AT&T, I
15 conclude that: the infrastructure described by the Klein Declaration and Klein Exhibits provides
16 AT&T Corp. with the capacity to assist the government in carrying out the Program; that the
17 infrastructure deployed included a data network (the [REDACTED] that apparently provided third
18 party access to the [REDACTED] room or rooms; that, if the government is in fact in communication with
19 this infrastructure, AT&T Corp. has given the government direct access to telecommunications
20 facilities physically located on U.S. soil; that, by virtue of this access, the government would have
21 the capacity to monitor both domestic and international communications of persons in the United
22 States; and that surveillance under the Program is conducted in several stages, with the early stages
23 being computer-controlled collection and analysis of communications and the last stage being
24 actual human scrutiny.

25 40. A key question is whether the infrastructure that AT&T deployed – which I refer to
26 for purposes of this declaration as the [REDACTED] *Configurations* – is being used solely for legitimate or

27 ¹³ Later in this Declaration, I provide my assessment of the volume of domestic and
28 international traffic captured.

1 *This deployment, however, is neither modest nor limited*, and it apparently involves considerably
2 more locations than would be required to catch the majority of international traffic.

3 44. The [REDACTED] Configurations are fully capable of pattern analysis, pattern matching and
4 detailed analysis at the level of *content*, not just of addressing information. One key component, the
5 [REDACTED], exists primarily to conduct sophisticated rule-based analysis of content. It is also
6 well suited to high speed data reduction – to the “winnowing down” of large volumes of data, in
7 order to identify only events of interest.

8 45. Klein Exhibit C speaks of a private [REDACTED] backbone network, which appears to be
9 partitioned from AT&T’s main Internet backbone, the CBB.¹⁵ This suggests the presence of a
10 private network. The most plausible inference is that this was a covert network that was used to
11 ship data of interest to one or more central locations for still more intensive analysis. I return to the
12 capabilities of the [REDACTED] Configurations later in this Declaration, under “Capabilities of the [REDACTED]
13 Configuration.”

14 46. Given the probable cost of these configurations, and the likely limited commercial
15 return, I find it exceedingly unlikely a financially troubled AT&T¹⁶ would have made these
16 investments at that time on its own initiative. I can envision no commercial reason, nor any
17 combination of commercial reasons, that would render that investment likely. I therefore conclude
18 that it is highly probable that funding came from an outside source, and consider the U.S.
19 Government to be the most likely source. This supports Mr. Klein’s assertion that the room was an
20 NSA secure room, accessible only to NSA-cleared personnel.

21 47. I also find that the components that were chosen are exceptionally well suited to a
22 massive, distributed surveillance activity (*see* “Capabilities of the [REDACTED] Configuration” later in this
23 Declaration). No other application provides as good an explanation for the combination of
24 engineering choices that were made.

25 48. In addition, the private [REDACTED] backbone network referred to in Klein Exhibit C,

26 ¹⁵ Klein Exh.C, pp 6, 12, 42. Again, *see* “Capabilities of the [REDACTED] Configuration” later in this
27 Declaration.

28 ¹⁶ I return to the topic of AT&T’s financial condition later in this Declaration, under “AT&T’s
Financial Condition in 2003.”

1 appears to be partitioned from AT&T's main Internet backbone, the CBB.¹⁷ This is perfectly
2 consistent with the notion of massive, covert distributed surveillance system. It is not consistent
3 with normal AT&T practice – they have been working for years to try to reduce the number of
4 networks in use, in the interest of engineering and operational economy.

5 49. For all of these reasons, I am persuaded that the [REDACTED] Configurations were deployed
6 primarily in order to perform surveillance on a massive scale, and not for any other purpose.

7 **BACKGROUND – FIBER OPTICS**

8 50. The Klein Declaration speaks (at ¶ 24 and in the sections following) of *splitting* the
9 light signal, so as to divert a portion of the signal to the [REDACTED] Room. It may be helpful to
10 review (at an informal level suitable for a non-specialist) some of the characteristics of fiber optic
11 transmission before proceeding.

12 51. Historically, electronic communications were carried over copper wires, or were
13 broadcast through the air. In both instances, it was often economically and technically
14 advantageous to *modulate*¹⁸ the signal onto a higher frequency wave. Doing so enables the
15 recipient to select from among multiple signals transmitted over the same physical medium. You
16 do this every time that you tune your television or radio to a particular channel.

17 52. More recently, fiber optics have supplanted the use of copper wire for many
18 applications, especially those involving long distances. Instead of modulating signals onto
19 electrical waves or radio waves, they are modulated onto light waves. Because light waves have a
20 much higher frequency than the waves used in copper wires, it is possible to modulate far more
21 information onto them.

22 53. Fiber optics have an additional advantage over copper wires: They do not generate
23 electrical interference, nor are they vulnerable to it. In addition, it is difficult to “tap” into a fiber

24
25 ¹⁷ Klein Exh.C, pp 6, 12, 42. Again, *see* “Capabilities of the [REDACTED] Configuration” later in this
Declaration.

26 ¹⁸ *Modulation* is “. . . the process of varying a carrier signal, typically a [signal in the shape of
27 a sine wave], in order to use that signal to convey information There are several reasons to
28 modulate a signal before transmission in a medium. These include the ability of different users
sharing a medium (multiple access), and making the signal properties physically compatible with
the propagation medium.” *See* <http://en.wikipedia.org/wiki/Modulation> (Exhibit H).

1 optic cable without detection. All of these characteristics are felt to make fiber more reliable and
2 more secure than copper.

3 54. At the same time, these characteristics mean that law enforcement has to work
4 harder to implement lawful intercept. The Hollywood image of an FBI agent with a pair of alligator
5 clips is a thing of the past.

6 55. This is one of the main reasons why CALEA obligates carriers to instrument their
7 networks in order to support requests for lawful intercept. Lawful intercept in today's world
8 depends on the cooperation of the carrier.

9 56. In this case, the splitter (described below) provides an equivalent function to that of
10 the alligator clips. However, instead of capturing traffic to a single target, these splitters
11 collectively transferred all or substantially all of AT&T's off net IP-based traffic¹⁹ (so-called
12 Internet *peering*²⁰ traffic to other Internet backbones) to a secure room.

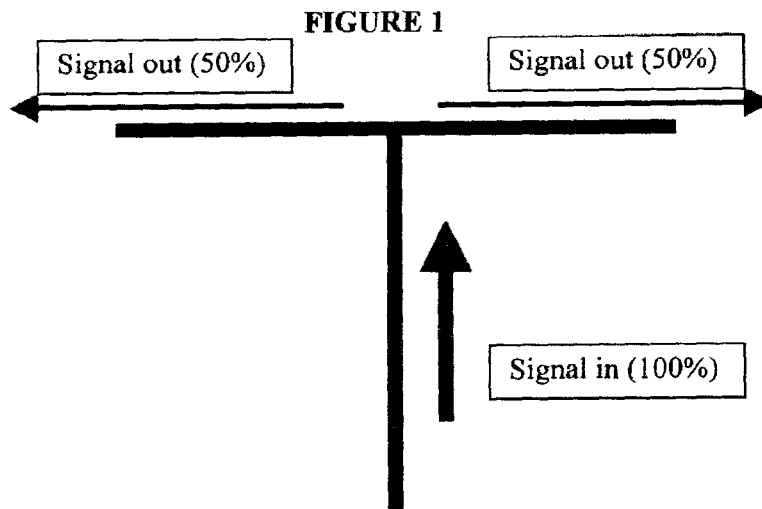
13 57. A splitter is a standard bit of optical gear. The simplest form is a "T" – one signal
14 comes in, two signals go out. The splitters in this case were 50/50 splitters, which is to say that they
15 split the signal such that 50% went to each output fiber. See the figure immediately below.

16
17
18
19
20
21
22
23
24

¹⁹ The basis for this statement is developed over the balance of this Declaration. Traffic from
25 one AT&T customer to another AT&T customer is *on net* traffic; traffic from an AT&T customer
26 to a customer of some other ISP is in general *off net* traffic. As previously noted, all Internet traffic
27 is *IP-based*, i.e. based on the Internet Protocol. I expand on this discussion in the section in which I
28 discuss "Traffic captured."

²⁰ Again, peering is the process whereby Internet providers interchange traffic destined for
their respective customers, and for customers of their customers.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



58. To the layman, it may seem strange that one can split a signal and still use both portions. In everyday life, if we divide something in half, each half is in some sense less than the whole. It is important to remember that, in this case, what is important is the bits (the information carried), not the underlying medium. This is more akin to making a copy of an audio CD – the CD that has been copied is not harmed by being copied. The copy contains the same information as the original.

59. Opto-electronic equipment is routinely designed to recover as much information as possible from weakened signals in order to attempt to compensate for *attenuation*²¹ (weakening, or loss of “punch”) of the signals over distance.

60. The AT&T designers were well aware that splitting the signal would make it weaker. They expected a loss of [REDACTED]²² as a direct result of splitting the signal in two, and a loss of an additional [REDACTED] due to possible inefficiencies in the process – think of this latter loss as being the equivalent of friction in a mechanical device. This makes for a combined loss of [REDACTED]. As long

²¹ “In telecommunication, *attenuation* is the decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path to the detector, but not including the reduction due to geometric spreading.” See <http://en.wikipedia.org/wiki/Attenuation> (Exhibit I).

²² dB is the standard abbreviation for decibel. “The decibel (dB) is a measure of the ratio between two quantities, and is used in a wide variety of measurements in acoustics, physics and electronics. . . . It is a “dimensionless unit” like percent. Decibels are useful because they allow even very large or small ratios to be represented with a conveniently small number. This is achieved by using a logarithm.” See <http://en.wikipedia.org/wiki/Decibel> (Exhibit J).

1 as the loss was less than [REDACTED], they presumably expected it to be within the normal operating
2 tolerances of the devices on both ends, so they apparently made no provision to correct for the loss.

3 [REDACTED]
4 [REDACTED]
5 [REDACTED] ²³

6 61. For the work that was described in the Klein Exhibits, each high speed circuit was
7 apparently comprised of multiple fiber optic cables. [REDACTED]

8 [REDACTED] to the splitters, and thereby to divert or copy the signals carried on those
9 circuits. They presumably chose not to connect the cables associated with other circuits to the
10 splitters, and thereby to refrain from diverting or copying the signals associated with those circuits.

11 62. [REDACTED] Configurations, [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED] ²⁴ This arrangement enabled the circuits to continue

15 to function just as they previously had, but also made the signals available to the [REDACTED]

16 63. The splitter configuration that AT&T used is routinely available from a major
17 supplier of equipment for electronic communications, [REDACTED]

18 [REDACTED]
19 [REDACTED]

20 **SUMMARY OF THE ARCHITECTURE OF THE [REDACTED] CONFIGURATION AND ITS**
21 **DATA CONNECTIVITY**

22 64. In this section, I provide a summary overview of the architecture of the [REDACTED]
23 Configuration and its data connectivity, based on the Klein Declaration, the Klein Exhibits, and my
24 professional expertise. More details are provided in later sections of this declaration.

25
26 ²³ See Klein Exh. A, p. 10.

27 ²⁴ [REDACTED]
28 [REDACTED]

1 65. The Klein Declaration refers to a "secret" room being constructed within AT&T
2 Corp.'s [REDACTED] Facility, called the "[REDACTED] Room." Klein Decl., ¶ 12.

3 66. While Mr. Klein worked at the [REDACTED] Facility, where he oversaw its
4 [REDACTED] room,²⁶ his duties included the installation of new fiber-optic circuits with
5 respect to AT&T's WorldNet Internet service.²⁷ Klein Decl., ¶¶ 15, 20.

6 67. In the course of his employment by AT&T, Mr. Klein reviewed the three documents
7 collectively referred to as the Klein Exhibits. Klein Decl., ¶¶ 25-26, 28.

8 68. The [REDACTED] Configuration, for purposes of my declaration and expert opinions,
9 includes the following basic elements: a room referred to in the Klein Declaration as the
10 [REDACTED] Room, [REDACTED] Room, [REDACTED] Room
11 [REDACTED] Room,
12 [REDACTED] sophisticated computers and other electronic devices located in or to be installed in this
13 room; sophisticated routers and switches capable of switching traffic among the computing systems
14 in the room, and also to other locations; and cables associated with data circuits entering and
15 exiting this room.

16 69. The [REDACTED] Room that Mr. Klein describes in his declaration is fully consistent
17 with the various [REDACTED] rooms referred to in the Klein Exhibits.

18 70. The Klein Exhibits describe procedures for splitting or diverting [REDACTED]
19 communications traffic associated with AT&T Corp.'s Common Backbone (CBB) fiber-optic
20 network by means of splitters²⁸ that fed into the [REDACTED] Room.

21 71. By following these procedures, all the communications carried on the associated
22 fiber optic circuits were diverted or copied to the [REDACTED] Room and could be made available
23

24 ²⁶ The [REDACTED] room and its equipment as described by Mr. Klein is a facility for
25 transmitting both domestic and international wire or electronic communications by
26 electromagnetic, photoelectronic or photooptical means. Klein Decl., ¶¶ 15, 19, 22.

27 ²⁷ The AT&T WorldNet Internet service provides its users with the ability to send or receive email,
28 to browse the web, and to send or receive other wire or electronic communications.

²⁸ I explained the function of a *splitter* earlier in this declaration, in the section on "Background –
Fiber Optics". [REDACTED]
[REDACTED] Room.

1 to any devices in that room.

2 72. With respect to the [REDACTED] Room in [REDACTED], the process resulted in the
3 diversion of all, or substantially all, of AT&T's [REDACTED] traffic at the [REDACTED]
4 facility to [REDACTED] equipment, with no significant adverse impact on AT&T's continuously operating
5 CBB Internet backbone.

6 [REDACTED] The figure below helps to clarify these relationships. [REDACTED]

7 [REDACTED]
8 Room.
9 [REDACTED]

10 Room.
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]

25
26 74. The Klein Exhibits also list equipment linked to or contained in the [REDACTED]
27 Room. These include sophisticated computers and other electronic equipment. See Klein Exh. C, p.
28 3 ("[REDACTED]"). At the same time, the Klein Exhibits do not indicate the quantities of

1 equipment, nor do they indicate the precise interconnections between them; consequently, the
2 connections depicted within the [REDACTED] Room in Figure 2 should be considered to be
3 suggestive but not necessarily exact.

4 75. An important group of devices in the [REDACTED] Room is the [REDACTED],
5 which is a [REDACTED] and the [REDACTED] Server.²⁹ As I explain in more detail
6 below, the [REDACTED] system is designed to apply logical tests to large volumes of data in real time. It is
7 well suited to the initial screening function of a comprehensive surveillance system – in fact,
8 surveillance is one of the system's primary functions.³⁰

9 76. The Klein Exhibits also refer to the [REDACTED] and to the [REDACTED]
10 circuit[s].³¹ Klein Exh. C, pp. 6, 12, 42. As I explain in more detail below, it is highly likely that
11 this [REDACTED] backbone provides a fiber-optic network connected to the [REDACTED] Room, but separate
12 and distinct from the CBB. In other words, while the [REDACTED] Room is connected to the CBB
13 (from which it receives communications), it is also connected to another network, and signals can
14 be sent out of or into the [REDACTED] Room over the [REDACTED].

15 77. In sum, the general architecture of the [REDACTED] Configuration is that communications on
16 the CBB are split by means of splitters in a splitter cabinet, and that these communications feed
17 into the [REDACTED] Room where they can be processed by the equipment in the [REDACTED]
18 Room. At the same time, the [REDACTED] provides a separate, two-way channel of
19 communication with the [REDACTED] Room. The documents reviewed do not, however, indicate
20 what entities can receive signals or information from or send signals or information into the [REDACTED]
21 [REDACTED] Room via the [REDACTED]. I consider it highly probable that one or more Centralized
22 Processing Facilities exist, as shown in Figure 2, but that belief is based on the nature of the job
23 that the [REDACTED] system is designed to do, rather than being based on the Klein Exhibits themselves.

25 ²⁹ See Klein Exh. C, p. 3 (“[REDACTED]”). The [REDACTED] is apparently implemented in
26 conjunction with a [REDACTED], possibly as software running on the [REDACTED].

27 ³⁰ [REDACTED]
28 ³¹ In the text, both the [REDACTED] backbone circuits and the [REDACTED] circuits are referred to in the singular. I believe that these are grammar errors on the part of the author, and that both should have appeared in the plural.

1 **CAPABILITIES OF THE SAN FRANCISCO [REDACTED] CONFIGURATION**

2 78. In this section, I explain my expert opinions about the activities likely to be
3 occurring in the [REDACTED] Room in [REDACTED].

4 79. In order to understand the capabilities of this configuration, it is particularly
5 important to understand the capabilities of the [REDACTED] and the
6 [REDACTED] website provides singularly little information about their offerings,
7 but a few public sources provide useful supporting detail, notably including a presentation that
8 [REDACTED] made to the [REDACTED], and a [REDACTED] presentation available on
9 the website of [REDACTED].³²

10 80. These devices are designed to capture data directly from a network, apply a
11 structured series of tests against the data, and respond appropriately. According to the [REDACTED]

12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]³³

20 81. Given the very high data rates that are supported, it is likely that many sophisticated
21 techniques are used to accelerate the processing.

22 [REDACTED] The [REDACTED] presentation on [REDACTED] web site³⁴ makes it clear that the [REDACTED] system
23 has the ability to inspect user application data (i.e. content), and not merely protocol headers. In
24 this context, it is worth noting that references to layer numbers reflect the [REDACTED]

25 ³² [REDACTED]
26 [REDACTED]

27 ³³ [REDACTED]

28 ³⁴ [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

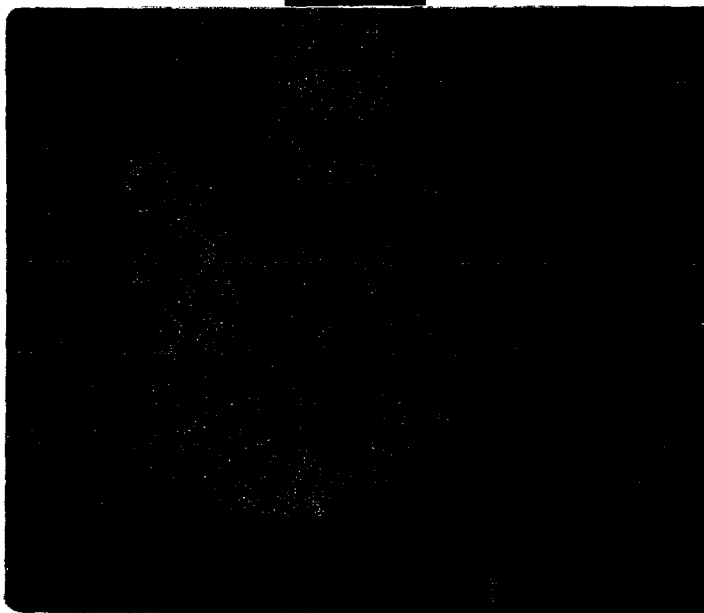
83. The statements in the [REDACTED] document make clear that the [REDACTED] system is well suited to process huge volumes of data, including user content, in real time. It is thus well suited to the capture and analysis of large volumes of data for purposes of surveillance.

84. The following figure, which is taken from the [REDACTED] presentation to [REDACTED], makes it clear that the system, in addition to its other capabilities, is designed to identify traffic of interest and to act on it. It has the ability to store interesting traffic to the onboard disk that is part of the system.

35 [REDACTED]

For a non-technical explanation of protocol layering in the context of the Internet, see section 2 of my paper "Evolving Core Capabilities of the Internet," Journal on Telecommunications and High Technology Law, 2004 (Exhibit G).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



85. In addition to its real time capabilities, the [REDACTED] offering can subsequently analyze large volumes of data in order to reconstruct session content as needed from the captured collections of packets. This would include e-mail, web browsing, voice over IP (VoIP), and other common kinds of Internet communication.³⁶

86. It would, in my judgment, be an error to evaluate the capabilities of this configuration – substantial though they are – solely on the basis of the equipment deployed by AT&T to the [REDACTED] Room. The AT&T documents clearly indicate the presence of an [REDACTED] network, apparently operating at [REDACTED].³⁷ This network, while much smaller than AT&T's CBB Internet backbone network, is nonetheless quite substantial.

87. The [REDACTED] backbone was logically distinct from the AT&T Common Backbone (CBB), but this does not necessarily mean that it had dedicated physical transmission facilities. It most probably operated over AT&T's standard optical fiber-based transmission systems, but using different high speed services – in effect, different circuits – than the CBB. If this network were carrying nothing more than a subset of AT&T's normal commercial traffic, they might not have

³⁶ [REDACTED]

³⁷ Klein Exh. C, pp. 6, 12, 42.

1 felt the need to do more – it has long been considered permissible to transmit *Sensitive but*
2 *Unclassified Information (SUCI)* over separate fiber-based transmission paths. Had there been
3 greater sensitivity about the data, it might have been protected in other ways, for instance by means
4 of link encryption.

5 88. The obvious and natural design for a massive surveillance system for IP-based data,
6 and the one most cost-effective to implement, would in my judgment be comprised of the
7 following elements: (1) massive data capture at the locations where the data can be tapped, (2) high
8 speed screening and reduction³⁸ of the captured data at the point of capture in order to identify data
9 of interest, (3) shipment of the data of interest to one or two central collection points for more
10 detailed analysis, and (4) intensive analysis and cross correlation of the data of interest by very
11 powerful processing engines at the central location or locations. The AT&T documents
12 demonstrate that equipment that is well suited for the first three of these tasks was deployed to [REDACTED]
13 [REDACTED] and, with high probability, to other locations. I infer that the fourth element also exists at
14 one or more locations.

15 89. Staff to analyze the data would probably be based at the central locations. There
16 would be no need to station analysts (as distinct from field support personnel) in the [REDACTED] rooms
17 where the data was collected. It is likely that the data were directly available for analysis by staff of
18 the agency that funded the [REDACTED] (which runs counter to normal practice in the case of
19 CALEA); otherwise, there would have been no need for a private [REDACTED], separate from the
20 CBB.

21 90. The [REDACTED] technology could potentially be used in a number of different ways, some
22 of which could be welfare-enhancing. The concern that must be raised in this case is that, in
23 conjunction with the diversion of large volumes of traffic described in the Klein Declaration and
24 the Klein Exhibits, this configuration appears to have the capability to enable surveillance and
25 analysis of Internet content on a massive scale, including both overseas and purely domestic traffic.
26

27
28 ³⁸ The [REDACTED] appears to be ideally suited to this role. It is, as previously noted, designed
to apply a large collection of tests against a huge volume of data at very high speed.

1 **TRAFFIC CAPTURED AT [REDACTED] ROOM**

2 91. In this section, I explain my conclusions about the volume and type of
3 communications traffic gathered by the [REDACTED] Room [REDACTED].

4 92. The Klein Declaration and Klein Exhibits B & C describe traffic diversions
5 associated with fiber-based circuits in the [REDACTED] facility.

6 93. All of the diverted data pertains to AT&T's Common Backbone (CBB), the IP-
7 based network that supports AT&T's Internet access customers, and that also carries AT&T's VoIP
8 services (voice over the Internet).³⁹ Nothing in the documents suggests that conventional telephony
9 traffic was diverted to the [REDACTED] Configuration.

10 94. The last page of Klein Exhibit B provides a list of CBB [REDACTED] (defined below)
11 links that were to be split and diverted to the [REDACTED] Configuration.

12 95. Nothing in the documents suggests that AT&T's *on net* traffic – traffic from one
13 AT&T customer to another – was diverted at the time. AT&T may at some point in time have
14 made some provision for its international customers (whose traffic to other AT&T customers
15 would also be on net), but the documents provide no guidance. My assumption is that on net traffic
16 was not diverted during the time frame to which the documents pertain.

17 96. Before proceeding, it is helpful to introduce and clarify some terms. *Peering* is the
18 process whereby Internet providers interchange traffic destined for their respective customers, and
19 for customers of their customers. The Network Reliability and Interoperability Council (NRIC), an
20 advisory panel to the FCC, defined peering in this way:⁴⁰

21 *Peering* is an agreement between ISPs to carry traffic for each other and for their
22 respective customers. Peering does not include the obligation to carry traffic to third

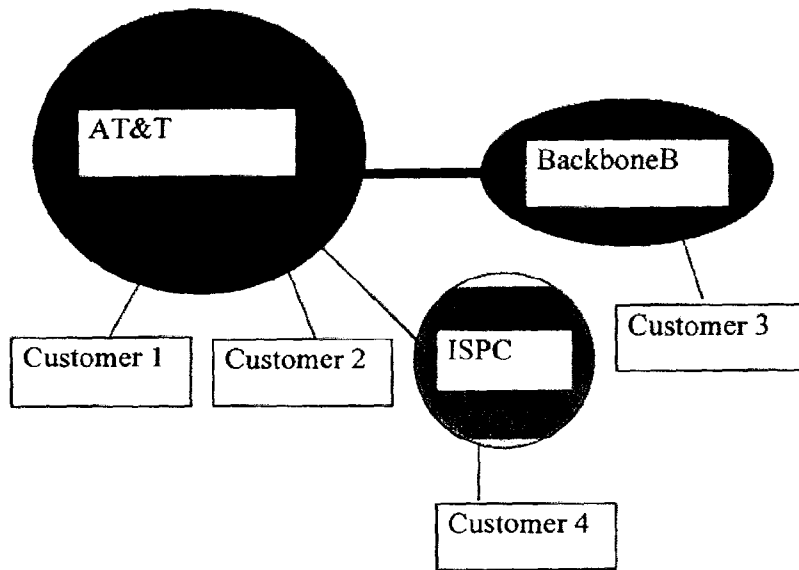
23 ³⁹ See *In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP*
24 *Telephony Services are Exempt from Access Charges*, FCC WC Docket 02-361, Petition of AT&T,
25 at 24 (filed Oct. 18, 2002), at
http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513386921
(Exhibit Q).

26 ⁴⁰ Report of the NRIC V Interoperability Focus Group, an advisory panel to the FCC:
27 "Service Provider Interconnection for Internet Protocol Best Effort Service," page 7, available at
http://www.nric.org/fg/fg4/ISP_Interconnection.doc (Exhibit R). See also chapter 14 of Marcus,
28 *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999
(Exhibit S).

1 parties. Peering is usually a bilateral business and technical arrangement, where two
2 providers agree to accept traffic from one another, and from one another's
customers (and thus from their customers' customers)

3 97. In the figure below, AT&T and Backbone B are *peers*. They have agreed to
4 exchange traffic for their respective customers. Traffic from AT&T customer 1 to AT&T customer
5 2 is *on net* traffic – it remains on AT&T's network. Traffic from AT&T customer 1 to customer 3
6 (a customer of backbone B) is *off net* traffic.

7 **FIGURE 4**



18 98. In the figure, ISP C is a *transit customer* of AT&T. ISP C pays AT&T to carry its
19 traffic, not only to AT&T customers, but to customers of other ISPs as well (such as, for example,
20 Customer 3). In the context of this discussion, AT&T can regard traffic from Customer 4 to
21 Customers 1 and 2 as being on net, in the sense that it does not traverse a peering connection.

22 99. It is perhaps also worth noting that AT&T and its peers and their many transit
23 customers do not merely connect to the Internet; rather they *are* the Internet. The Internet is not a
24 single, huge and over-arching network, but rather a collection of independent networks that
25 collectively comprise a worldwide communications stratum.

26 100. Again, the last page of Exhibit B provides a list of CBB [REDACTED] that were to
27 be split and diverted to the [REDACTED] Configuration. The sizes of these circuits are listed,
28 with some at [REDACTED], some at [REDACTED], and some at [REDACTED]. These

1 are all quite substantial circuits – the [REDACTED] are apparently on a par with the largest circuits that
2 were in widespread use in AT&T’s CBB Internet backbone at the time.

3 101. Traffic to and from several very large Internet providers at that time [REDACTED]
4 [REDACTED] was delivered over OC-48 circuits. Traffic to and from
5 another group of large providers [REDACTED]
6 [REDACTED] was delivered over [REDACTED] circuits. Traffic to and from smaller, but still quite substantial,
7 providers [REDACTED] was delivered over [REDACTED] circuits.

8 102. Large Internet backbone providers typically use direct interconnects (private
9 peering) to exchange traffic with their largest “trading partners in bits,” the firms with which they
10 exchange the largest volume of traffic. For providers where the volume of traffic exchange at some
11 location is large enough to warrant peering arrangements, but not large enough to justify the cost of
12 a separate circuit for private peering, it is customary instead to interconnect with multiple peers at a
13 so-called “public peering point” in order to exchange traffic with multiple providers there.⁴¹ AT&T
14 was connected to [REDACTED]
15 [REDACTED]
16 [REDACTED] configuration.

17 103. At the point where I left Genuity in July 2001 (some eighteen months before these
18 splitters were deployed), I was intimately familiar with our traffic exchange patterns with other
19 providers. Our measurement instrumentation ranked with the very best in the industry at that time.
20 It is possible to draw many inferences about traffic flows among other providers from one’s own
21 traffic exchanges.

22 104. Based on my experience at Genuity, I believe that the traffic that was diverted
23 represented all, or substantially all, of AT&T’s peering traffic in the [REDACTED]

24 105. I base my reasoning on the knowledge of Genuity’s peering traffic patterns, and on
25 my general understanding of peering traffic patterns in the industry. As of July 2001, our three
26 largest peers were WorldCom, AT&T and Sprint, collectively representing 50-60% of our traffic.

27 ⁴¹ See Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*,
28 Addison Wesley, 1999, pages 280-282 (Exhibit S).

1 Our next largest peering partners changed somewhat over time, but typically included Qwest,
2 Level3, Verio and Cable and Wireless. Public peering points such as MAE-West represented a
3 small and steadily diminishing percentage of our peering traffic. AT&T had a larger customer base
4 than Genuity, but one might expect the relative proportions to be generally similar, with the
5 obvious exception of AT&T's traffic to itself. The relative sizes of peering circuits on the last page
6 of Klein Exhibit B is not inconsistent with this assumption. Genuity had peering arrangements with
7 50 to 60 networks, but many of them exchanged relatively little traffic with us. All of our
8 significant peering partners at that time appear on the list on the last page of Klein Exhibit B.

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

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

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

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

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

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

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

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

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

4 **NUMBER OF LOCATIONS**

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

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

13 115. Klein Exhibit B talks about general AT&T naming conventions, and says: [REDACTED]

14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 ⁴³ This emphasis on a standardized, cookie-cutter approach is consistent with AT&T standard practice, but also implies a
18 planned deployment to multiple sites, surely more than two or three.

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

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

⁴³ Klein Exh. B, p. 4.

1 location.

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

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

16 **TRAFFIC CAPTURED BY MULTIPLE [REDACTED] ROOMS**

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

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

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

27
28 ⁴⁴ This is the same methodology used in my paper with Laffont, Tirole and Rey. Exhibit D, pp. 373-74.

1 on net for a variety of reasons.

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

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

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

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

24
25 ⁴⁵ See remarks of Hossein Eslambolchi, AT&T labs president and chief technology officer, quoted
26 in BroadbandWeek Direct at <http://www.broadbandweek.com/newsdirect/0208/direct020802.htm>,
27 August 2, 2002 (“AT&T has been steadily growing its backbone traffic and now expects to surpass
28 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.

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

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

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

12 **ALTERNATIVE REASONS WHY AT&T MIGHT HAVE DEPLOYED THE [REDACTED]**
13 **CONFIGURATIONS**

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

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

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

24 131. Second, AT&T might have deployed the [REDACTED] configurations in order to sell security
25 services to their customers. AT&T does in fact offer a service called Internet Protect to its Internet
26 access customers, and the service appears to be based on the [REDACTED] offering. Indeed, this is the
27
28

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

4 132. This explanation also falls short. The [REDACTED] Configurations were deployed beginning
5 in early 2003, meaning that planning was probably under way six to twelve months earlier, given
6 AT&T process. Internet Protect was not announced until March, 2004.⁴⁹ Aside from that, AT&T
7 officials themselves characterized aspects of Internet Protect as something that they had already
8 deployed for other purposes, and only belatedly realized might benefit their customers.⁵⁰ All
9 indications are the Internet Protect was an attempt to extract commercial value from a deployment
10 already made – or more likely, from a new deployment using the same technology as the [REDACTED]
11 Configuration – rather than having been the original rationale for the deployment.

12 133. Third, it is possible that AT&T might have deployed the [REDACTED] configuration in order
13 to meet obligations for lawful intercept. The [REDACTED] system can be used for this purpose; however, it
14 is not credible that this was the rationale for the deployment. Far simpler and far less expensive
15 solutions could have met all the limited CALEA requirements that were in force at the time of
16

17 ⁴⁷ [REDACTED]

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

25 ⁴⁹ <http://www.att.com/news/2004/03/22-12972> (Exhibit W).

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

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

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

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

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

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

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

24 139. The ██████ Configuration is, at a technical level, an excellent fit with the requirements
25

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

28 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/>.

