

1 CINDY COHN (SBN 145997)
cindy@eff.org
2 DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
3 KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
4 ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
5 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
6 San Francisco, CA 94109
Telephone: (415) 436-9333
7 Fax: (415) 436-9993

8 RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
9 LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street, Suite 650
10 San Francisco, CA 94104
Telephone: (415) 433-3200
11 Fax: (415) 433-6382

12
13 Attorneys for Plaintiffs
14
15

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

16 UNITED STATES DISTRICT COURT
17 FOR THE NORTHERN DISTRICT OF CALIFORNIA
18 OAKLAND DIVISION

19)
20 CAROLYN JEWEL, TASH HEPTING,)
YOUNG BOON HICKS, as executrix of the)
21 estate of GREGORY HICKS, ERIK KNUTZEN)
and JOICE WALTON, on behalf of themselves)
22 and all others similarly situated,)
23 Plaintiffs,)
24 v.)
25 NATIONAL SECURITY AGENCY, *et al.*,)
26 Defendants.)

CASE NO. 08-CV-4373-JSW

Declaration of Dr. Brian Reid

The Honorable Jeffrey S. White

1 I, Brian Reid, declare as follows:

2 1. I have been asked by plaintiffs' counsel to apply my expertise and experience in
3 network operation and engineering to examine and analyze the evidence described herein. In this
4 declaration, I describe my background, outline my conclusions, and explain the basis and the
5 reasoning that support those conclusions. If called as a witness, I could and would testify to the
6 matters stated herein.

7 2. Based on my expertise, after carefully reviewing all of the documents in this case, I
8 believe it is very likely that the plaintiffs' communications passed through the peering site at
9 AT&T's Facility at 611 Folsom Street at least once during the 17 years at issue in this case, and
10 that these communications—along with the rest of the traffic passing over all of the peering-link
11 fibers into which splitters were installed at AT&T's 611 Folsom Street Facility—were replicated,
12 with one replica copy redirected by the optical splitter assemblies described by Mark Klein and the
13 other sent to its original destination. Based on the documents reviewed, and my expertise in
14 network engineering, it is virtually impossible for me to imagine a scenario in which this did not
15 happen.

16 **BACKGROUND**

17 3. I am a telecommunications and data-networking expert with over 40 years of
18 experience studying, developing, operating, and improving communications systems. I have
19 extensive knowledge of and experience with international telecommunications infrastructure and
20 the technology regularly used for lawful surveillance pursuant to warrants and court orders. I have
21 been involved in the development of several critical Internet technologies, including email, web,
22 and document representation and transmission.

23 4. I am currently the Director of Operations at Internet Systems Consortium (ISC), an
24 organization that develops and distributes internet software and uses that software to operate
25 critical infrastructure. We meet payroll by offering support contracts for the use of our free
26 software. ISC also participates in the development of standards for the internet and is a significant
27 contributor to the Internet Engineering Task Force.

1 5. I have worked at ISC for over 13 years. In my current role as Director of
2 Operations, which I have held for almost three years, I have management and lead technical
3 responsibility for ISC's server and network operations, staff IT, and for one of the 13 clusters of
4 DNS root servers that serve the entire internet, worldwide. I was previously a Senior Member of
5 Technical Staff in the Office of the Chief Technical Officer (CTO), where I was the sole employee
6 in the office and essentially carried out the duties of CTO: I took part in every technical and
7 business decision made at ISC and reported directly to the company president. When it was
8 needed, I served as the Director of Corporate Communications (I am an experienced writer and
9 editor), and as the Director of Operations and Engineering.

10 6. I received a Bachelor of Science in Physics from the University of Maryland in
11 1970. While obtaining my undergraduate degree, I worked for the University of Maryland
12 Computer Science Department as a Systems Programmer, where I developed operating system
13 software and compiler for the Univac 1100 series of computer, funded by NASA. I also produced
14 the software for one of the ALSEP research modules on Apollo 17 (the Lunar Surface Gravimeter).

15 7. After graduating from the University of Maryland, I worked in the airline industry
16 on scheduling software for four years before joining Carnegie Mellon University as a research
17 scientist in 1974. In 1975, I entered graduate school at Carnegie Mellon, and was awarded a PhD in
18 Computer Science in 1980. My dissertation research developed the Scribe word processing system,
19 for which I received the Association for Computing Machinery's Grace Murray Hopper Award in
20 1982. Most scholars consider Scribe to be the inspiration for HTML, which is the *lingua franca* of
21 the World Wide Web.

22 8. From 1980 to 1987, I was an assistant professor of electrical engineering at
23 Stanford University. In 1984, I was a recipient of the National Science Foundation's Presidential
24 Young Investigator Award. While at Stanford, I conducted research regarding the university's
25 connection to the Internet, and developed system architecture for VSLI (very-large-scale
26 integration) systems, including the SUN workstation [Stanford University Network], which was a
27 modular personal computer system designed for use in an Ethernet-type local network. While I was
28 at Stanford, malicious actors first began showing up on the internet, and I was involved in or took

1 the lead in every attempt by Stanford and its law enforcement partners to locate the evildoers and
2 stop them.

3 9. In 1987, I joined Digital Equipment Corporation (DEC), as a Consulting Engineer at
4 the Western Research Laboratory (WRL). While working at WRL, I worked with Paul Vixie to
5 develop one of the first connections between a corporate network and the Internet, known as
6 "Gatekeeper." The protection techniques we developed evolved into what is now called a network
7 "firewall." I taught classes in internet technology to large numbers of DEC employees, and helped
8 the corporation build its internal internet. Former New York Times reporter John Markoff told me
9 that when the FBI arrested computer hacker Kevin Mitnick in 1995, he was carrying false
10 identification saying that he was me. (The book *Takedown* describes this arrest).

11 10. In 1995, after working in WRL for eight years, I was promoted to Director of my
12 own DEC research group, the Network Systems Laboratory (NSL). Under my leadership, NSL
13 developed the first independent Internet exchange point as the Internet became available for
14 commercial use in the 1990s. An independent exchange point is one that is not owned or controlled
15 by any of its users, in much the same fashion that an airport is not owned or controlled by any of
16 the airlines that use it. My laboratory also led the company-wide project to build one of the first
17 Web search engines. My Network Systems Laboratory was responsible for making our search
18 engine fully accessible to the entire internet.

19 11. In 1999, I joined Bell Labs Research Silicon Valley (BLRSV), a startup venture of
20 Lucent Technologies, as Laboratory Director. Under my leadership, BLRSV developed affordable
21 fiber to the home (FTTH) technology, which provided unprecedented high-speed internet access
22 via the installation and use of optical fiber from a central point directly to individual buildings such
23 as residences, apartment buildings, and businesses.

24 12. When Lucent collapsed in 2001, I joined Carnegie Mellon University as a Professor
25 of the Practice of Computer Systems at the University's nascent Silicon Valley branch, located at
26 the NASA Ames Research Center at Moffett Federal Airfield in Mountain View, California.
27 During my time as a professor at Carnegie Mellon Silicon Valley, I conducted research and
28 infrastructure management and worked with NASA on networking technology for the International

1 Space Station and on developing a multi-disciplinary, multi-institutional High-Dependability
2 Computing Program (HDCP) to improve NASA's capability to create and operate dependable
3 software.

4 13. In 2002, I joined Google as the Director of Operations. The primary focus of my job
5 responsibilities had to do with Google's networking capabilities.

6 14. In 2004, I left Google to become a self-employed consultant.

7 15. In 2005, I joined my current employer, ISC, as the Director of Operations and
8 Engineering.

9 16. The conclusions that I draw below are based on on my professional training and
10 experience, in addition to the following information, as explained in more detail below: the Privacy
11 and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to
12 Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Section 702 Report"); the
13 AT&T documents attached to the Declaration of Mark Klein; the facts and events personally
14 observed by Mr. Klein, as set forth in his declaration (but not the conclusions he draws from those
15 facts and events described); the facts and events personally observed by James Russell, as set forth
16 in his declaration (but not the conclusions he draws from those facts and events described).

17 17. One of the AT&T documents (Ex. C to the Klein Declaration, "Study Group 3
18 LGX/Splitter Wiring, San Francisco /Issue 1, 12/10/02," at p. C-3) lists a number of devices. The
19 Russell declaration states that these devices are present at AT&T's 611 Folsom Street Facility. I am
20 familiar with and have first-hand knowledge of nearly all of the listed devices. (I have no first-hand
21 knowledge of Narus systems but have read the documentation that was available at the time).

22 18. I am not receiving any compensation for my work as an expert in this matter.

23 **SUMMARY OF CONCLUSIONS**

24 19. My conclusions can be summarized as follows:

25 20. First, the technological setup at 611 Folsom Street, San Francisco, as described in
26 the AT&T documents and in Mr. Klein's declaration, copies and redirects all communications
27 passing over all of the peering-link fibers into which the splitters were installed.
28

1 21. Second, it is very likely that plaintiffs’ communications passed through a peering
2 link at AT&T’s 611 Folsom Street Facility at least once during the 17 years at issue in this case.
3 Communications pass through peering links when they travel from one network to another, *e.g.*,
4 from AT&T to Verizon or Sprint. But the precise route that communications take as they travel
5 from network to network vary; internet routing is not static. Because of the volatile nature of
6 internet routing, and because many email communications are routed over temporary routes chosen
7 by a router, it is unfathomable to me that in 17 years, at least one of plaintiffs’ communications did
8 not travel via the peering links described in the AT&T documents at the 611 Folsom Street
9 Facility, a major Internet peering point. The same is true for a peering link at any other major
10 peering point.

11 22. Third, it is likely that plaintiffs’ communications—along with the rest of the traffic
12 passing over all of the peering-link fibers into which splitters were installed at AT&T’s 611
13 Folsom Street Facility—have been copied and redirected by optical splitter assemblies described
14 by Mr. Klein in his declaration. This is because:

15 a. What Mr. Klein describes is a technological setup that *passively* copies all
16 traffic passing over all of the peering-link fibers into which the splitters were installed. The optical
17 splitting device described by Mr. Klein does not and cannot study the contents of a transmission to
18 make a decision about whether to copy it. The splitter copies everything. The brand of splitter
19 noted in Mr. Klein's declaration does not even use electricity. It is purely optical.

20 b. It would not make sense to use an active device such as a router or switch to
21 do inline searching of every communication routed through it because of cost and performance
22 issues. The number of such devices needed would be in the hundreds or even thousands, and they
23 would slow down all traffic.

24 c. Monitoring the “to” and “from” addressing information in an email, along
25 with the subject line and email body, requires first capturing and reassembling most of the body of
26 the email. This means that, in order to search for “selectors,” the NSA architecture must capture
27 and reconstitute an entire transaction (message or group of messages) before analyzing any of it.
28 As explained below, the PCLOB Section 702 Report confirms that the NSA captures the entire

1 contents of an email message, even if they intend to look only at its “to,” “from,” or “subject line”
2 information.

3 23. Fourth, conducting surveillance at the peering connections between AT&T’s
4 “Internet backbone” and non-AT&T Internet providers is consistent with surveillance aimed at
5 “one-end foreign” communications.

6 **EXPLANATION OF THE BASIS FOR MY CONCLUSIONS**

7 **Certain Network Infrastructure Is Required To Send Information And** 8 **Communications Over The Internet.**

9 24. Internet transmission systems are extremely complex. There are many thousands of
10 pages of documentation on how it all works, hundreds of textbooks to assist learning, and often a
11 new technology requires revising an existing specification. This section is therefore just a brief
12 outline of how information travels over the internet. Explanations of network operation usually
13 reference the “ISO 7-layer model,” whose formal name is “ISO/IEC 7498-1,” which is a
14 conceptual model for thinking about, characterizing and standardizing the different functions
15 necessary for a telecommunication or computing system, without regard to its underlying structure.
16 Wikipedia notes ISO/IEC 7498-1 “is a conceptual model that characterizes and standardizes the
17 communication functions of a telecommunication or computing system without regard to its
18 underlying internal structure and technology. Its goal is the interoperability of diverse
19 communication systems with standard protocols.”¹ The specification of the ISO 7-layer model
20 predates the development of the internet. The ISO 7-layer model is thus described as a good way to
21 talk about networks but no longer a suitable way of building them. Despite there not being an exact
22 match between the vocabulary of the ISO 7-layer model and the architecture of the internet today,
23 because the different functions necessary for a computing system remain the same.

24 25. When an email message is sent, it moves first from the sender’s computer to a mail
25 server. That mail server locates the recipient’s mail server and initiates a transmission of the
26 email’s data stream to the recipient. Messages, such as emails, must be formulated into a layer-4
27

28 ¹ Wikipedia, “OSI model,” https://en.wikipedia.org/wiki/OSI_model (last updated Sep. 6, 2018).

1 stream (pursuant to the Transmission Control Protocol, or TCP). As part of the delivery process,
2 this layer-4 stream is divided into individual packets, each transmitted separately. When the
3 packets are presented to the next layer, the routing layer (layer 3), the routing devices (routers)
4 choose the “next hop” of the transmission path based on their routing tables (which are used to
5 determine where data packets traveling over a network will be directed). That hop delivers the
6 packet to another router, which uses its own routing tables to continue to move the packet closer to
7 its destination. At the time a packet is transmitted via these routers, there is no central control and
8 no global specification of the path to be taken. Misconfigured routers can cause packets to be
9 routed in circles, never to reach their destination.

10 26. The most important concept for this declaration is that, on the internet, routers
11 (networking devices) determine the path taken by a packet—not circuits. This is an important
12 distinction between the Internet and phone networks. Circuits are discrete (specific) paths between
13 two or more points along which signals can be carried over the internet. Although there are actual
14 circuits (usually fiber optic circuits) involved in the Internet, and although data is ultimately
15 transmitted over those circuits, these circuits do not have any involvement in determining the path
16 taken by a packet. This is a job performed only by routers, and they can decide to send different
17 packets along different routes/circuits. Because routers are aware only of their connections to the
18 “next hop” and not of any global end-to-end path, it is theoretically possible (though unlikely) for
19 each packet in a transmission to take a different path to their mutual destination.

20 27. Next, the routing device presents the packets to the next layer, the network layer
21 (layer 2). If a layer-3 device (*e.g.*, a router or server) presents to a layer-2 network (*e.g.*, a fiber link
22 or an ethernet) a packet that is too large for it, the layer-2 device is expected to divide that
23 overlarge packet into fragments (each of which meets its size limitation) and transmit each
24 fragment separately. The ultimate recipient must reassemble fragments into packets before the
25 packets can be reassembled into a data stream. Different fragments can be routed over different
26 paths across the internet.

27 28. There are two fundamentally different approaches to network reliability. Neither has
28 a formal name but they are often described in classrooms and conference halls as “fortification or

1 agility” or “strength vs flexibility.” You can build a network so that each component is as strong
2 and reliable as you know how to make it, or you can build a network whose components are
3 adequately strong and adequately reliable but count on nimbleness in the software to re-route data
4 away from broken devices and damaged connections. Internet engineers usually refer to this re-
5 routing phenomenon by saying “the internet routes around damage.” In combat situations it is very
6 difficult to destroy an internet-technology communication system by destroying its components,
7 because surviving components will find a path that does not traverse the damaged component.

8
9 29. It is very difficult to track the path taken by a particular packet. There are test
10 procedures (“traceroutes”) that will send probe packets and report the path they took, but traceroute
11 says nothing about the path taken by a previous packet, or that will be taken by the next packet.

12 30. The sender of an email can neither specify nor determine the hop-by-hop routing
13 path taken by the packets comprising that data stream initiated when they send their message. In
14 the vocabulary of the internet, the creation of this routing path is called “making a TCP connection
15 to the recipient.” A TCP connection has very little in common with, say, a telephone connection,
16 because the creation of a TCP “connection” does not involve reserving resources along the
17 transmission path or even establishing a transmission path. If the transmission path were fixed at
18 the time that the sending began, reliability would suffer because it would not be possible for the
19 intermediate routers to make changes to that path to bypass failure or link saturation. (It does cause
20 the recipient *mail server* to reserve resources for the inbound stream data, which makes it accept
21 data faster).

22 31. The bottom layer (layer 1), is the physical layer. This layer is responsible for
23 sending bits across circuits. The term “internet backbone” has been used colloquially, including by
24 the media, the PCLOB, and courts (including the Court and parties in this case), to refer to the
25 long-haul circuits (usually fiber optic circuits) of individual large-scale ISPs like AT&T. The term
26 harkens back to the early days of the internet, in the 1980s, when a single network, the National
27 Science Foundation Network (NSFNET), linked together supercomputing centers at research and
28 academic institutions across the country. In 1994, the Clinton Administration decommissioned
NSFNET and privatized the network, handing the job of carrying long-distance internet traffic over

1 to various commercial firms. For the convenience of the Court, I use “internet backbone” in that
2 colloquial sense for purposes of this declaration.

3 32. Because optical fibers are small and relatively fragile, they are encased in multiple
4 layers of strong protective material. Because the installation of fiber optic cable is very labor-
5 intensive, the installers usually buy cables with dozens or hundreds of individual fiber strands. It is
6 a huge amount of work to lay a fiber optic cable on the ocean floor, so installers want that cable to
7 have as many strands as circumstances permit. It is common to see land-based fiber optic cables
8 with 768 strands. Undersea cables necessarily have many fewer strands (one recent high-
9 performance transpacific cable has 6 strands); this is because the undersea cables must have signal-
10 boosting amplifiers at intervals along the ocean floor, and those amplifiers require electric power.
11 The electric power must be piped in from one of the ends of the cable. This imposes practical
12 limitation. Because 6 strands used directly are not enough to meet huge and growing transmission
13 requirements if each fiber were to carry only a single transmission channel, fiber operators
14 multiplex numerous transmissions in one strand using different colors of light (a process called
15 Wave Division Multiplexing, or WDM).

16 33. Wave Division Multiplexing of unrelated transmission channels puts a big burden
17 on a would-be wiretapper. If you want to tap a fiber-optic cable to look for certain kinds of traffic,
18 you must not only access the optical signal, you must demultiplex it into its component wave-
19 divided channels. Like most electronic technology, WDM devices are improving, but at the
20 beginning of the time frame we are discussing, 12-channel WDM multiplexors on long fiber
21 strands were common. The owner of the fiber can send 12 times as much data over it, but the
22 would-be wiretapper must demultiplex the channels to extract those of interest. If all 12 WDM
23 channels are of interest, it normally takes 12 monitoring devices to watch them all. As we have
24 noted previously, packets and fragments that are part of the same email stream transmission can be
25 routed over different paths using different fibers and/or different wavelengths of that fiber. Putting
26 a tap at the point where an undersea cable reaches land is certainly possible, but it is much more
27 complex than putting a tap in some place where the ISP has already done the work of
28 demultiplexing.

1 34. Unless all parties to a communication are customers of the same ISP, then at some
2 point a transmission must be handed from the sender's ISP to the recipient's ISP. ISP's have
3 historically been suspicious and untrusting of one another, and creating a link between two of them
4 required difficult negotiations. No ISP wanted to put equipment on a competitor's premises.
5 Locations that did not belong to any ISP, used only for the purpose of interconnection, were
6 originally called NAPs (Network Access Points). If two ISPs connected at a NAP and each saw the
7 other as being approximately its peer in size and capacity, then they would sign a "peering
8 agreement" whereby neither would charge for the handoff. If one ISP was much larger than the
9 other, then the larger ISP would usually refuse to "peer," instead requiring that the smaller ISP
10 become its customer instead of its peer. Within 5 years after this type of agreement became
11 common, the vocabulary had evolved. All of it was called "peering," and the vendor/customer
12 relationship was called "paid peering." People stopped calling these facilities NAPs and started
13 calling them "peering points." Peering points are the buildings where "peering links" are located.
14 Today, even the term "paid peering" is unusual. It is all called "peering"; sometimes money
15 changes hands and sometimes it does not.

16 35. The Privacy and Civil Liberties Oversight Board (PCLOB) Report's phrase "the
17 flow of communications between communication service providers" is a description of peering
18 links.²

19 36. If both the sender and recipient of an email message use large ISPs, then a single
20 connection between those two ISPs might be sufficient to deliver the message. The sender's ISP
21 routes the message to the closest facility where it peers with the recipient's ISP, and hands it off to
22 them at that peering point. But if either or both of the parties to a communication use smaller ISPs,
23 or overseas ISPs, then the path between them is complicated enough to require multiple handoffs at
24 multiple peering points. I have seen situations in which 9 ISPs and 8 peering-point handoffs are
25 involved in the transmission of one email message. Since AT&T is a large ISP, it is not unusual for
26 email messages to transit its network even when neither the sender nor the recipient is an AT&T
27

28 _____
² PCLOB Section 702 Report, at 35.

1 customer. AT&T provides internet service to a large number of other companies, many of which
2 connect at peering points.

3 **The Technological Setup Of AT&T's 611 Folsom Street Facility Copies And Redirects All**
4 **Communications Passing Over All Of The Peering-Link Fibers Into Which The Splitters**
5 **Were Installed.**

6 37. The AT&T documents establish (Ex. B to the Klein Declaration, "SIMS Spitter Cut-
7 In and Test Procedure OSWF Training, Issue 2," at p. B-20) that AT&T's 611 Folsom Street
8 Facility served as a "Service Node Routing Complex" (SNRC) (AT&T's phrase for a "peering
9 point," a facility in which peering connections are made) where AT&T's telecommunications
10 network "peered" with the following internet networks: ConXio, Verio, XO, Genuity, Qwest,
11 Allegiance, Abovenet, Global Crossings, C&W, UUNET, Level 3, Sprint, Telia, and PSINet.
12 AT&T's 611 Folsom Street Facility also peered with circuits to two Internet Exchange Points,
13 MAE-West (Metropolitan Area Exchange, West) and PAIX (Palo Alto Internet eXchange).

14 38. According to Mr. Klein's declaration, he personally observed a "splitter cabinet"
15 during his work as a technician at AT&T at the 611 Folsom Street Facility, because he and one
16 other technician were required to connect new fiber optic circuits to the "splitter cabinet." He also
17 testified that starting in February 2013, the "splitter cabinet" split the light signals that contained
18 the communications in transit to and from the internet networks listed in the previous paragraph

19 39. In the course of preparing this declaration, I independently analyzed the AT&T
20 documents and the statements made by Mr. Klein in his declaration. I do not rely on Mr. Klein's
21 description of them. For purposes of this analysis I accept as true the statements made in his
22 declaration describing how the splitters operated, what peering points they were connected to, and
23 that they created a complete copy of the light signals crossing those peering points, as these are all
24 facts within his personal knowledge and observation. I do not rely on any further conclusions Mr.
25 Klein drew from those facts he observed; instead, I analyze those facts independently. AT&T
26 Director of Asset Protection Russell testified that the documents attached to Mr. Klein's
27 declaration are authentic AT&T documents, and I accept this testimony as true.

1 40. While I was an employee Lucent, as the Laboratory Director of Bell Labs Research
2 Silicon Valley, while exploring Lucent’s optical products, I discovered the splitter devices
3 described in the Mr. Klein’s declaration in a catalog and then went to see one in person at Lucent's
4 headquarters in New Jersey. I read all of Lucent’s documentation on the splitter devices at that time
5 and am familiar with the technology.

6 41. A “splitter” is a communication device that accepts one input and produces
7 multiple outputs, each being a replica of the input. They are almost universal in cable TV
8 installations: the inbound TV cable is connected to a splitter, each of whose outputs being
9 connected to some device that uses the cable TV signal. An optical splitter has the same function: it
10 accepts one inbound beam of light and produces two or more outbound beams of light. The
11 splitters described by Mr. Klein are ADC 50/50 units (referred to in the ADC catalog as 1x2
12 splitters), accept one inbound optical fiber connection and deliver two outbound optical fiber
13 connections, each of which has a (slightly diminished) copy of the input. If the transmission being
14 monitored is carried over a wire, then an electrical splitter must be used. If the transmission being
15 monitored is carried over a fiber optic cable strand, then an optical splitter must be used.

16 42. The machinery at AT&T’s 611 Folsom Street Facility described in the AT&T
17 documents and in Mr. Klein’s declaration collected all communications passing over all of the
18 peering-link fibers into which the splitters were installed, and any other new circuits on which he
19 installed splitters.

20 43. The AT&T documents describe a secret, private “backbone” network separate from
21 the public network where normal AT&T customer traffic is carried transmitted.

22 44. The AT&T documents also explain that the fiber optic cables were cut, and that
23 fiber optic splitters were installed at the cut point.

24 45. The AT&T documents describe a system with massive, real-time surveillance
25 capabilities. For example, it includes a NARUS 6400, a computer that can:

- 26 • Simultaneously analyze huge amounts of information based on rules provided by
27 the machine operator.

- 1 • Analyze the content of messages and other information, not just headers or routing
- 2 information.
- 3 • Conduct the analysis in “real time,” rather than after a delay.
- 4 • Correlate information from multiple sources, multiple formats, over many protocols
- 5 and through different periods of time in that analysis.

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

11 47. This infrastructure is capable of monitoring all traffic passing through the fiber optic
12 cables connected to the splitters at the peering point (some of it not even from AT&T customers),
13 including voice-over-IP (VoIP), data, fax, whether international or domestic. This does not include
14 non-VoIP voice going over the 4ESS switches, or AT&T to AT&T (within network)
15 communications, which would not pass through the peering links.

16 **It Is Highly Likely That Plaintiffs’ Communications Traveled Through the**
17 **“Backbone”-to-Network Peering Link at the AT&T 611 Folsom Street Facility.**

18 48. Because internet routing is so volatile, and because many email communications
19 will be routed over temporary routes chosen by a router, it is unfathomable to me that in 17 years,
20 at least one of plaintiffs’ communications did not travel via the peering points at AT&T’s 611
21 Folsom Street Facility, a major Internet peering point. The same is true for any other major peering
22 point. It is thus highly likely that plaintiffs’ communications traveled through the peering link at
23 the AT&T 611 Folsom Street peering point.

24 49. For plaintiffs who are AT&T internet customers, it is even more likely, given that
25 their communications would have travelled over AT&T’s network so frequently. Anytime an
26 AT&T customer sends a communication over the internet to a non-AT&T customer, that
27 communication has to pass through a peering point with another network.
28

1 50. It is still highly likely, even for plaintiffs who were not AT&T internet customers,
2 that their communications traveled through the peering link at the AT&T 611 Folsom Street
3 peering point, as a function of communication with AT&T customers. Anytime a non-AT&T
4 customer sends a communication over the internet to an AT&T customer, that communication has
5 to pass through a peering link from another network to the AT&T network.

6 51. This is particularly true for individuals located in San Francisco and Los Angeles,
7 given the high likelihood that their communications—whether to or from an AT&T customer—
8 would be routed through the San Francisco peering link.

9 52. Whenever a data path develops problems (from overload, damage, equipment
10 failure, etc.) the routers instantly compute a new path and adjust packet routing accordingly. There
11 is potential for any traffic to pass through any node as a result of automatic temporary re-routing.

12 53. Real-time routing decisions are so common, and the routers are routing so many
13 packets, that recording dynamic and temporary changes to network routing would be a burden. It is
14 therefore not customary to keep logs or records of those dynamic re-routing decisions.

15 54. Routers normally do not have mass storage such as hard drives, so any record-
16 keeping of real-time routing decisions would require sending data from the router to a logging
17 device. This would decrease the routing capacity of the router. As a result, I am not aware of any
18 ISP anywhere that keeps records of its dynamic routing updates—except during specific (and rare)
19 diagnostic events.

20 **It Is Highly Likely That The Plaintiffs' Communications Have Been Copied And**
21 **Redirected By The Splitter Assemblies Described By Mr. Klein.**

22 55. Choosing what to copy and what not to copy involves significant amounts of
23 computing and database access. If a splitter is inserted in an internet data path, it would be very
24 burdensome on that ISP if the computations of what to copy or not copy took place inline. The only
25 reasonable process is to make a copy of everything and send it to an external system that would
26 decide what to keep and what to discard. All of the communications that pass through a monitored
27 fiber are copied and redirected. Some device then reconstitutes the individual transactions and
28 decides which ones to keep and which ones to discard.

1 56. As a result, it is likely that at least one of plaintiffs' communications were copied
2 and redirected by the splitter assemblies described by Mr. Klein, along with all of the
3 communications passing over the peering-link fibers into which the splitters were installed.
4 Perhaps plaintiffs' communications were not retained after they were analyzed, but they were
5 certainly in the possession of the NSA until that analysis was completed.

6 **(A) Mr. Klein describes a technological setup that passively copies all traffic over the**
7 **peering links—not a system that monitors traffic to determine what to copy and**
8 **what not to copy.**

9 57. It is standard practice for companies that move data around as a business to
10 purchase devices with computing resources that are a little bigger, but not a lot bigger, than they
11 will need on the two days out of the year when they expect the most daily traffic—peak times.
12 Monitoring and deciding whether to make a copy of a communication at that scale inside an
13 electronic device, such as a router, would require using a significant portion of the device's
14 computing resources, and thus throwing away the purchased computing capacity to conduct
15 monitoring. This would cause the device to run slower, and if you didn't purchase a device with
16 enough computing power, there would be an overload at peak times. Since no one in the industry
17 uses routers to analyze data for monitoring, I have no source of data from which to quote numbers.
18 However, based on knowledge of what computer chips are inside a router and what computer chips
19 are inside a computer, I believe that it is safe to say that placing an email monitoring function
20 inside a router would use 90% of the capacity of that router. All modern high-capacity routers
21 perform "cut-through routing," which means that the routing decisions are made by the peripheral
22 device controllers and not by the main router's central processing unit (CPU). Any content analysis
23 would require disabling cut-through routing and referring all inbound traffic to the router's central
24 computer, which by itself would cause a 50% slowdown.

25 58. There is significant innovation in the computer industry, and newer devices tend to
26 be cheaper. The particular hardware and software used to copy and redirect communications
27 transiting AT&T's peering links in Northern California and elsewhere may have changed over the
28 years, but the factors requiring the basic architecture to copy and redirect Internet communications

1 transiting those peering links for further filtering and analysis is economic and not technical.
2 Evolution in monitoring technology does not affect my conclusion that plaintiffs' communications
3 were copied and redirected by the splitters.
4

5 **(B) Monitoring “to” and “from” addressing information from an email in transit**
6 **requiring first capturing and reassembling the entire email, including the**
7 **message contents.**

8 59. Monitoring the “to” and “from” addressing information in an email requires first
9 capturing and reassembling most of the body of the email. The demarcation in an email message
10 between its header and body is just a textual blank line, and you cannot find that blank line without
11 assembling all of the message to that point.

12 60. Message assembly is done from packets, and packets typically have more than 1000
13 characters in them, sometimes more.

14 61. To find the boundary between the “to” and “from” addressing information and the
15 body of the message it is necessary to capture as much as 1500 characters of the message payload,
16 and these characters must correspond to part of the message that includes the “to” and “from”
17 addressing information. The PCLOB Section 702 Report, however, states, “If a single discrete
18 communication within an MCT [multiple communications transaction] is to, from, or about a
19 Section 702–tasked selector, and at least one end of the transaction is foreign, the NSA will acquire
20 the entire MCT.”³ This means that the NSA architecture captures and reconstitutes an entire
21 transaction (message) before analyzing any of it, because if it did otherwise, it would not need to
22 acquire the entire MCT once it had acquired the segment of interest. This means that the NSA has
23 captured the entire contents of an email message even if they intend to look at its “to” and “from”
24 addressing information.

25 ///

26 ///

27 ///

28 ///

³ PCLOB Section 702 Report, at 39.

1 **Conducting Surveillance at the Peering Links Between AT&T’s**
2 **“Internet Backbone” and Non-AT&T Internet Providers Is Consistent With**
3 **Surveillance Aimed At “One-End Foreign” Communications.**

4 62. Conducting surveillance by copying and redirecting communications in the manner
5 described by the AT&T documents and Mr. Klein’s testimony is consistent with surveillance aimed
6 at “one-end foreign” communications transiting the “Internet backbone.”

7 63. First, capturing the raw contents of an intercontinental fiber does not ensure that you
8 will capture all desired communication. If you wait until other devices have merged and
9 reassembled the fragments of the communication (some of which might have been routed over
10 different fibers from others) you can be much more confident that you are capturing the intended
11 communications. By the time the communications devices have merged and reassembled the
12 fragments of international traffic into messages that can be analyzed, significant domestic traffic
13 will necessarily have been combined with it.

14 64. Second, as described above, because every router involved in a message
15 transmission makes its own decisions about the next hop in the message’s journey, a router may
16 determine that the best path for a San Francisco to Dallas transmission is to route it via Tokyo.
17 Given that Internet service providers routinely store email message contents all over the world,⁴
18 this is a relatively common phenomenon. Given the way information is routed over the Internet,
19 using a splitter to copy all communications traveling across a node and then redirecting those
20 communications in the manner described by the AT&T documents is a logical and unsurprising
21 approach in order to ensure that all one-end foreign communications are captured. The PCLOB
22 Section 702 Report says that the NSA conducts “technical measures, such as IP filters . . . to
23 prevent the intentional acquisition of wholly domestic communications.”⁵ IP filters are only
24 necessary because the peering links do not contain only one-end-foreign communications, but also

25
26 _____
27 ⁴ ISPs store email messages while they wait for you to check your mail. What it means to “check
28 your mail” is that you instruct your computer to contact the server computer on which your ISP
stores your mail. ISPs do not normally reveal the location of such computers.


⁵ PCLOB Section 702 Report, at 41.

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

wholly domestic communications. It is logical and unsurprising for such IP address filtering to occur after a splitter to copy all communications traveling across a node.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

DATE: September 27, 2018



Brian Reid