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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **Declaration of Professor Matthew Blaze** The Honorable Jeffrey S. White

I, Matthew Blaze, declare as follows:

1. I have been asked by counsel for plaintiffs to apply my expertise and experience to examine and analyze evidence described below. After setting forth my background, I summarize my conclusions and then explain the basis and the reasoning supporting my conclusions. If called as a witness, I could and would testify to the matters stated herein.

2. Based on my expertise, and after carefully reviewing all of the documents in this case, I believe it is highly likely that the communications of all plaintiffs passed through peering-link fibers connected to the splitter (and thus the splitter itself) that Mark Klein describes at the AT&T Folsom Street Facility. From a technical perspective, the interception architecture described in the AT&T documents and in Klein's declaration is a logical and unsurprising approach for a high-volume bulk interception operation, including interception targeting "one-end-foreign" communications.

BACKGROUND

3. I am currently employed a full professor of computer and information science at the University of Pennsylvania, in Philadelphia, where I teach graduate and undergraduate classes, conduct research, and handle various administrative matters. The focus of my research is on computer and network security, cryptography, surveillance and interception technology, and related subjects. However, I make this declaration entirely on my own behalf.

4. In 1993, I received my PhD in computer science from Princeton University. The focus of my dissertation was networking and large scale distributed systems.

5. Since 2004, I have held my current position on the faculty at the University of Pennsylvania. From 1992 through 2004, I was a member of the research staff at AT&T Laboratories in New Jersey (known for part of that period as AT&T Bell Laboratories). While at AT&T, I conducted research and led research projects in computer and network security, cryptography, surveillance and interception technology, and other topics. (I note that this declaration does not rely on any proprietary information entrusted to me during my employment at AT&T.)

6. Over the course of my career, I have produced over 100 publications related in some way to my research in computer security, networking security, cryptography, and/or surveillance. These include scholarly-refereed journal articles, refereed conference papers and workshop papers, as well as standards documents, written testimony, and articles such as op-eds in the popular press. This includes one scholarly-refereed journal articles that I co-authored with Steven M. Bellovin, Susan Landau, and Stephanie K. Pell, entitled, "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law," published in Vol. 30 of the Harvard Journal of Law in 2016, which outlines in detail the network architecture of the Internet.[1]

7. I have been engaged as an expert in various litigation matters related to my expertise from time to time, most often in patent cases. I have testified in deposition numerous times and at trial approximately five times.

8. In addition to my professional training and conclusions, I have relied on the following information, as explained in more detail below: Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014) ("PCLOB Section 702 Report"); the Foreign Intelligence Surveillance Court order issued on October 3, 2011, for the interception of Internet content on October 3, 2011 ("FISC Oct. 3, 2011 Opinion"); the Foreign Intelligence Surveillance Court order issued on September 25, 2012, released by the government as a result of FOIA litigation with the American Civil Liberties Union ("FISC Sept. 25, 2012 Opinion"); the Classified Declaration of Deborah A. Bonanni, National Intelligence Agency Deputy Director (Dec. 20, 2013) ("NSA Deputy Dir. Fleisch Classified Decl."); the Section 702 Congressional White Paper entitled "The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act" ("FISA White Paper"); the AT&T documents attached to the Declaration of Mark Klein; the facts and events personally observed by Klein, as set forth in his declaration; and an the facts and events personally observed by James Russell, as set forth in his declaration. I do

[1] Steven M. Bellovin, Matt Blaze, Susan Landau, Stephanie K. Pell, *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016).

not rely on the conclusions Klein or Russell draw from those facts and events described in their declarations; instead I have conducted my own analysis of those facts and events.

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

SUMMARY OF CONCLUSIONS

10. My conclusions can be summarized as follows:

11. First, assuming the splitter described by Mr. Klein (or similar technology) exists as described, it likely copied and redirected plaintiffs' communications.

12. Second, to extract the "to" and "from" fields from email messages transiting the Internet (what the government calls "Internet metadata") it is necessary to first acquire the entire contents of the message. This is because the "to" and "from" fields are found in the same communications layer as the content of the email message.

13. Third, conducting surveillance at the peering connections between AT&T's Internet backbone and non-AT&T Internet providers is consistent with Privacy and Civil Liberties Oversight Board (PCLOB) and Foreign Intelligence Surveillance Court (FISC) disclosures about the government's Internet surveillance.

14. Fourth, conducting surveillance at the peering connections between AT&T's Internet backbone and non-AT&T Internet providers is consistent with surveillance aimed at "one-end foreign" communications.

EXPLANATION OF THE BASIS FOR MY CONCLUSIONS

How Communications Travel On The Internet

15. The Internet is a packet-switching network. That means that communications are broken into small packets, each of which may be routed a different way through the communications network. The packets are then reassembled at the communications endpoint, where they are received as, for example, an email, video, or webpage.

16. In the conventional description, computer network technology is organized as a "stack." From the bottom down, the "layers" are physical, link (or data link), network, transport, and application. The layer names come from the reference architecture of the Open Systems Interconnection (OSI) standard. The layers are often referred to by number, rather than by name

(e.g., the physical layer is "layer 1"; the link layer is "layer 2"; and so on). Though the OSI protocols, which predate the Internet, are now largely defunct, the terminology has lived on even though it is not a perfect match for today's Internet architecture. For example, while the OSI standards included 7 layers, two additional layers than those listed above, on the internet there are no equivalents to OSI layers 5 (a session layer) and 6 (a presentation layer); some of the layer 6 functionality, however, often appears as part of layer 7 (the application layer). Given the history behind the development of modern day internet networking standards, there continues debate amongst network engineers about the precise number of layers to include in descriptions of how information travels across the Internet and the precise terminology used to describe these layers, but the functionality remains the same.

17. Each layer in the stack offers a specific set of services (provided via software) to the layer immediately above it, and requests services from the layer below it. As information travels across the Internet, these services are typically carried out via a string of digital devices: a layer on one device talks to the corresponding layer on the next device. These services are not provided in the network but on the "edges." Data in the application layer (OSI layer 7), and transport layer (OSI layer 4) are not processed by intermediate routers in the Internet. The communications in the application and transport layers are end-to-end communications from Host A (the originating or "source" computer) to Host B (the receiving or "destination" computer). For example, web servers and email servers are not generally part of the Internet infrastructure itself, but rather are provided by ordinary computers at the "edge" of the Internet, generally operated parties other than the ISP.

18. Different protocols govern the communications between layers and between devices on the same layer.

19. The top layer, the application layer, supports application and end-user processes. The application layer provides the basis for e-mail forwarding and storage. It allows a user to pass information to a network. For example, the software application that you type an email into using your computer and the software application displaying it on the other end function at the application layer. The application layer uses a variety of different protocols.

20. The transport layer accepts data from the application layer, splits it up into smaller units, passes these data units (also called "packets" or "datagrams") to the network layer, and ensures that all the pieces arrive at the other end. It also reassembled packets on the other end by putting data back together in the correct order. These services are conducted via the Transmission Control Protocol ("TCP"). TCP, for example, will retransmits any packets are dropped by the next layer, the network layer, during transmission to ensure that all packets necessary to reconstruct the data sent arrive at the destination computer. At the transport layer, a packet includes a TCP header, which includes a port numbers, which act as the internal address within the destination computer. It is fundamental to the design of the Internet that TCP headers are end-to-end; they are not processed by intermediate routers in a network. This means that the contents of the TCP header are created by one end system and are relevant only to the computer at the other end of the connection. Unlike the network layer, intermediate routers do not ordinarily examine or otherwise rely on TCP headers. In other words, the data transmitted with TCP and in the TCP header is not, from an Internet design perspective, shared with other parties. The only true party to TCP communications is the destination computer at the other end of the connection. As far as the network is concerned, TCP headers are just unexamined content.

21. The network layer accepts packets from the transport layer and routes and delivers those packets from source to destination across multiple networks. Gateways—such as router, firewall, server, or others device that enables traffic to flow in and out of a network—function at the network layer. The network layer uses the Internet Protocol ("IP") to route and deliver packets. At the network layer, each packet includes a "header" that describes what the packet is, along with where the packet is going and where it came from, in the form of Internet Protocol addresses (or "IP addresses). Whereas a port number more or less is similar to a room in a building, an IP address is similar to the building's address.

22. The information contained within packet headers—whether the IP header or the TCP header—is distinct from the "to," "from," and "subject line" information contained within an email. The "to," "from," and "subject line" information of an email can be viewed only at the application layer, *after* packets are reassembled via TCP/transport level. As a result, IP-based

communications render content/non-content distinctions in email functionally meaningless. Networks—and specifically, the routers and the links that connect them—are concerned solely with packet delivery from a source IP address to a destination IP address, and not the contents of the packet.

23. The link, or data link, layer provides the protocol mechanisms needed to send and receive packets on a single network. The link layer first forms "frames" (or protocol data units") from the packets it receives from the network layer and sequentially transmits the frames to the physical layer. The link layer creates frames by dividing the streams of bits received from the network layer into manageable data units, typically a few hundred or few thousand bytes. The link layer then transfers these frames between adjacent network nodes (or "peering links") in a wide area network (WAN), a computer network that extends over a large geographical distance/place, or between nodes on the same local area network (LAN) segment, a computer network that interconnects computers within a limited area such as a residence, university campus, or courthouse, such as a Wi-Fi or Ethernet. Each frame has a header, describing, for example, the source Ethernet address and the destination Ethernet address. (Just as with IP and TCP headers, the information contained within a frame header is completely distinct from the "to," "from," and "subject line" information contained within an email.) The receiver typically confirms correct of each frame by sending back an acknowledgement frame.

24. The lowest layer of the stack, the physical layer, cover the physics of communication: the radio frequencies used, the voltages for traditional Ethernet, the electrical or optical properties of the physical connection between a device and the network or between network devices, and more. This layer has no concern for the meaning of the bits; it deals only with the setup of physical connection to the network and with transmission and reception of signals.

25. On the receiving end, the reverse happens. The physical layer provides bits to the link layer, which reconstructs packets via frames. The network layer accepts the packets from the link layer, and then, using the IP address information contained with the packet header, routes and delivers those packets to the destination address. The transport layer, via TCP, accepts the packets

and reassembled them, putting the data together in the correct order so that it may be displayed in human-readable form via the application layer.

26. Internet Service Providers (ISPs) provide service at the Network Layer discussed above by routing the packets to their destinations. All Internet service providers, including AT&T, route traffic for variety of parties, including the inbound and outbound traffic for their own customers coming from or going to other computers on the Internet connected to other ISPs. AT&T also serves as what is known as a "backbone" provider, handling traffic not only for its own customers, but also "transit" traffic passing between other Internet service providers. It is through large backbone providers such as AT&T that local Internet service providers are able to connect their customers to the entirety of the Internet. The effect is that the packets passing within AT&T's network (including in the San Francisco office) will include three kinds of traffic: that being routed between two AT&T customers, that being routed between AT&T customers and those of other ISPs, and that being routed between one ISP and another ISP. All three kinds of traffic would be expected to have been included on split links sent to the NSA room in the San Francisco office.

Given The Inherent Structure Of The Internet, Collecting "To" And "From" Addressing Information From Emails In Transit Requires Capturing All The Packets Related To The Email And Reassembling The Entire Email.

27. Given the inherent structure of the Internet outlined above, there is no way to view or collect the "to" and "from" addressing information from an email messages by packet interception without first reconstructing the email message content by reassembling the contents of all of the relevant packets.

28. The outdated conception of a bright line between content and addressing information (which is sometimes referred to as "metadata") originates from early phone networks. Originally, metadata was a reference to the dialing, routing, addressing, and signaling (DRAS) information utilized in the Public Switched Telephone Network (or "PSTN").

29. Unlike the Internet, which is a packet-switched network, the traditional telephone network is a circuit-switched network, in which each communication builds a circuit that it uses exclusively for the duration of a call. And unlike the Internet's architecture, where the intelligence

is at the edges (in the connected computers, rather than in the network itself), in the phone network, the intelligence is centralized in the telephone company's infrastructure: the phone switches. As the only elements of that network with any sophistication, the phone switches must receive and process all signaling information (encoded as tones or dial pulses) to complete calls. At the time of the development of the telephone network, this design was a practical necessity: the phones of the time were very simple devices with no computing or storage capability, and rotary dial phones were almost completely electromechanical save for a few passive electronic components.

30. The essential architecture of the phone network was designed at a time when putting any but the most basic functions in telephones was technically and economically infeasible. The phone network's design meant that most services had to be provided by the telephone companies, and the phone companies could offer only rudimentary services to their customers—notably dialing or answering a phone call. Requesting a service was easy: you took the phone off the hook and listened for a dial tone. You then dialed the number and the phone system (rather than the user's phone) would do all the subsequent work needed to complete the call.

31. Given the rudimentary communications model of the phone network, it was plausible for the courts to draw a bright line between content (a conversation, or perhaps a modem session) and metadata (DRAS information). Even by 1979, however, as advanced features started to appear in the phone network, the line content and addressing information began to blur.

32. IP-based communications, in contrast, render the content/non-content distinctions functionally far less meaningful.

33. For example, in the phone system, "addressing" is straightforward: it is the task of specifying to the network the destination of a call, and an "address" is "a unique 10-digit number assigned to a main station, *i.e.*, a phone number. On the Internet, the link, network, transport, and application layers all have their own identifiers—and none of these identifiers include the email address listed in the "to" or "from" fields in an email. From a technical perspective, the "to" and "from" information, along with the subject line and the text within the body email, is *all* content information, because, as described above, it can only be viewed at the application layer, after content has been extracted and reassembled from the packets.

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

34. As noted above, the Internet backbone is a complex network of communication links over which traffic is routed. A "splitter," as used in this case, is a device that optically "splits" all communication on a link between two network nodes, creating an second link that can be connected to a third node. This effectively copies all the traffic on the original link to the third node, while leaving the traffic undisturbed between the original two nodes. It is, in effect, a specialized device for physically "wiretapping" the kinds of high-speed optical communication links that make up the Internet backbone.

35. Klein testifies he personally observed and operated the splitter, and for purposes of this analysis I accept his description of how the splitters operated, what peering-link fibers they were connected to, and that the copied, as these are all facts within his personal knowledge and observation. I do not rely on any further conclusions Mr. Klein drew from those facts he observed; instead, I analyze those facts independently.

36. I independently analyze the AT&T documents and do not rely on Klein's description of them. I accept AT&T Director of Asset Protection Russell's testimony that they are authentic AT&T documents.

37. The system described by the AT&T documents and Klein's personal observations does the following: "Taps," via splitters, backbone communication links in the AT&T San Francisco facility, routing a copy of the traffic on these links to a secure room controlled by the National Security Agency (NSA).

38. From a technical perspective—given that extracting the "to," "from," subject line, and text within the body of emails requires reconstructing all packets that comprise an email—this interception architecture, in which all the traffic passing across peering-link fibers is copied via a splitter and then filtered separately, is a logical and unsurprising approach for a high-volume bulk interception operation. An alternative approach would involve scanning for and copying the desired traffic in the ISP's routing infrastructure itself. But such an approach would require significant changes on the part of the ISP, and could potentially degrade the ISP's performance,

especially when large volumes of traffic are to be intercepted. Another approach (common used for lawful interception of email by law enforcement) would dispense with the need for any packet interception by obtaining the data from the operators of the targeted users' mail servers. However, this approach requires the active cooperation of the various mail server operators, many of which, for international users, are located outside the jurisdiction of the United States.

39. It is highly likely that the communications of all plaintiffs passed through the link connected to the splitter (and thus the splitter itself) that Klein describes.

40. As the Internet "routes" communications through the network, the particular links through which a packet travels to its destination is a function of the state of the network at the precise instant a packet is sent, rather than an attribute of a particular connection.

41. It is my understanding based on the available evidence that the AT&T San Francisco peering-link fibers to which the splitter was attached carried a high concentration of the international and domestic Internet traffic passing through the AT&T San Francisco facility. That means that the link connected to the splitter would, in turn, have access to a large fraction of the traffic passing through the facility. This would include Internet traffic of AT&T's customers—including traffic of plaintiffs who are AT&T Internet customers—as well as peering traffic of customers of other ISPs who communicate online with AT&T customers.

42. Pursuant to the inherent architecture of the Internet, in order for a communication from an AT&T customer to reach a non-AT&T customer, that communication has to pass through a peering point with another network. Likewise, a communication from a non-AT&T customer to an AT&T customer must has to pass through a peering point with another network.

43. For those plaintiffs who are AT&T Internet customers, there is even more of a likelihood that their communications passed through the node connected to the splitter (and thus the splitter itself) that Klein describes, given that they would have been on AT&T's network so frequently. But it still highly likely that plaintiffs' communications passed through the link connected to the splitter (and thus the splitter itself) that Klein describes, even if they were not AT&T Internet customers, as a result of communicating with AT&T customers.

44. The fact that all plaintiffs reside in either northern California or southern California also increases the likelihood that their communications passed through the node connected to the splitter (and thus the splitter itself) at the AT&T San Francisco facility, given the proximity of the San Francisco peering site and the high concentration of the international and domestic Internet traffic passing through it.

45. The AT&T documents also suggest that there are similar splitter systems at other AT&T facilities. If that is true, then that would only increase the odds that plaintiffs' communications passed through peering-link fibers to which splitters were installed at AT&T peering points.

46. It would not be surprising if the particular hardware and software used to copy and redirect communications transiting AT&T's peering links in Northern California and elsewhere has changed over the years. But as long as the basic architecture copies and redirects Internet communications transiting those peering links for further filtering and analysis, my conclusion that plaintiffs' communications are likely subject to the initial copying and redirection remains valid.

Copying And Redirection Of Plaintiffs' Communications At AT&T's Peering Links Is Consistent With The PCLOB's Description And Other Government Disclosures Of The NSA's Interception Of Internet Content For Purposes Of Selector Searching.

47. The use of splitters or similar technology to copy and redirect communications transiting Internet backbone peering links as disclosed by the AT&T documents and Klein's testimony is consistent with the disclosures by the Privacy and Civil Liberties Oversight Board (PCLOB). The PCLOB states that the government's interceptions occur "with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit." PCLOB Section 702 Report, at 7.

48. The PCLOB further states:

a. The NSA "intercepts communications directly from the Internet 'backbone.'" *Id*. at 124.

b. The interceptions are of "communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the 'Internet backbone.'

The provider is compelled to assist the government in acquiring communications across these circuits." *Id*. at 36-37.

c. "The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet." *Id*. at 39.

d. "[U]pstream collection acquires 'Internet transactions,' meaning packets of data that traverse the Internet, directly from the Internet 'backbone.'"

e. The interceptions occur "in the flow of communications between communication service providers." *Id*. at 35. That is a description of "peering links."

49. Other government disclosures also confirm that interceptions of Internet backbone communications are occurring: "[T]he NSA collects electronic communications with the compelled assistance of electronic communications service providers as they transit Internet 'backbone' facilities within the United States." NSA Deputy Dir. Fleisch Classified Decl., at 25. "NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States." FISA White Paper, at 3.

50. The Foreign Intelligence Surveillance Court (FISC), similarly confirms "the acquisition of Internet communications as they transit the 'internet backbone' facilities[.]" FISC Sept. 25, 2012 Opinion, at 26.

51. These descriptions are consistent with the splitters described by the AT&T documents and Klein that copy and redirect communications transiting peering links between AT&T's backbone and other Internet providers.

Conducting Surveillance At The Peering Connections Between AT&T's Internet Backbone And Non-AT&T Internet Providers Is Consistent With Surveillance Aimed At "One-End Foreign" Communications.

52. Conducting surveillance by copying and redirecting communications in the manner described by the AT&T documents and Klein's testimony is consistent with surveillance aimed at "one-end foreign" communications transiting the Internet backbone.

53. The PCLOB states: "Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet

communications, what is referred to as the 'Internet backbone.' The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702-tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector." PCLOB Section 702 Report, at 36–37.

54. The PCLOB further states that the NSA uses "technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States." PCLOB 702 Report, at 38. The NSA employs these "technical measures, such as IP filters . . . to prevent the intentional acquisition of wholly domestic communications." *Id*. at 41.

55. IP filters are necessary only because the communications links the government monitors *do* contain wholly domestic communications, in addition to one-end-foreign communications. Otherwise they would not need to be filtered out.

56. From a technical perspective, the interception architecture described in the AT&T documents and Klein declaration is consistent with the NSA's goal of conducting surveillance on "one-end foreign" communications, because use of a splitter to copy all communications traveling across a node ensures that all one-end foreign communications are captured, so that the NSA may then conduct IP filtering. IP filtering at other places in the network itself would likely degrade the ISP's performance.

57. Further evidence that the communications links the government monitors do contain wholly domestic communications is the fact that, as the FISC has noted, "NSA's upstream collection devices will acquire a wholly domestic 'about' [communication] if it is routed internationally." FISC Oct. 3, 2011, at 34.

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

DATE: September 28, 2018

Matthew Blaze