

1	UNITED STATES PATENT AND TRADEMARK OFFICE
2	BEFORE THE PATENT AND APPEAL BOARD
3	PALO ALTO NETWORKS,)
4	INC.,)
5	PETITIONER,)
6	v.)
7	CENTRIPETAL NETWORKS,)
8	INC.,)
9	PATENT OWNER.)
10	
11	
12	
13	DIGITALLY-RECORDED MOBILE VIDEOCONFERENCE
14	DEPOSITION OF JON B. WEISSMAN, taken remotely
15	before Cheryl A. Rooney, RPR, CRR, Online General
16	Notary Public within and for the State of Nebraska,
17	Beginning at 9:01 AM CT, on August 19, 2022.
18	
19	
20	
21	
22	
23	
24	
25	

1	APPEARANCES
2	(Appearing Remotely)
3	THE WITNESS:
4	JON B. WEISSMAN
5	(Appearing Remotely)
6	FOR THE PETITIONER:
7	MR. SCOTT A. MCKEOWN
8	ROPES & GRAY
9	2099 Pennsylvania Avenue, NW
10	Washington, DC 20006-6807
11	(202) 508-4600
12	scott.mckeown@ropesgray.com
13	and
14	MR. ANDREW RADSCH
15	MS. KEYNA CHOW
16	ROPES & GRAY
17	1900 University Avenue
18	6th Floor
19	East Palo Alto, CA 94303-2284
20	(650) 617-4000
21	andrew.radsch@ropesgray.com
22	keyna.chow@ropesgray.com
23	
24	
25	

1	APPEARANCES
2	(CONT'D)
3	(Appearing Remotely)
4	FOR THE PATENT OWNER:
5	MR. JEFFREY H. PRICE
6	KRAMER LEVIN NAFTALIS & FRANKEL LLP
7	1177 Avenue of the Americas
8	New York, NY 10036
9	(212) 715-9100
10	jprice@kramerlevin.com
11	and
12	MS. JENNA FULLER
13	KRAMER LEVIN NAFTALIS & FRANKEL LLP
14	333 Twin Dolphin Drive
15	Suite 700
16	Redwood Shores, CA 94065
17	(650) 752-1728
18	jfuller@kramerlevin.com
19	and
20	MR. CRAIG W. KRONENTHAL
21	BANNER & WITCOFF
22	71 South Wacker Drive
23	Suite 3600
24	Chicago, IL 60606
25	(312) 463-5000
	ckronenthal@bannerwitcoff.com
	ALSO PRESENT
	VIDEOGRAPHER:
	MR. GUY WHITE (Appearing Remotely)
	Thomas & Thomas Court Reporters
	1321 Jones Street
	Omaha, Nebraska 68102
	(402)556-5000 FAX (402)556-2037

1	I N D E X		
2	CASE CAPTION.....	Page	1
3	APPEARANCES.....	Page	2
4	INDEX.....	Page	3
5	TESTIMONY.....	Page	4
6	REPORTER CERTIFICATE.....	Page	66
7	DIRECT EXAMINATION:		
8	By Mr. Price.....	Page	4
9	EXHIBITS		
10	EXHIBITS PREVIOUSLY MARKED:	IDENTIFIED	
11	Exhibit 1001 Centripetal Patent '856		13
12	Exhibit 1003 Weissman Declaration		13
13	Exhibit 1004 Buru Patent '795		13
14	Exhibit 1005 Baehr Patent '231		14
15	Exhibit 1029 Centripetal v. Cisco		
16	Case No. 2:18-cv-00094		
17	(E.D. Va.), Dkt. No. 548		
18	(June 10, 2020 Trial		
19	Transcript)		63
20			
21			
22			
23			
24			
25			

Page 5 1 (Whereupon, the following proceedings 2 were had, to-wit:) 3 THE VIDEOGRAPHER: Good morning. 4 We are now on record. My name is Guy White. 5 I'm recording this deposition on behalf of 6 Thomas & Thomas Court Reporters. 7 The deponent for today's deposition is 8 Dr. Jon Weissman. 9 The date is August 19, 2022. The 10 approximate time is 9:01 a.m. central time. 11 This deposition is being conducted via 12 Zoom with some or all of the parties appearing 13 remotely. Do the parties agree the witness may 14 be sworn in remotely? 15 MR. PRICE: Yes. 16 MR. MCKEOWN: Yes. 17 THE VIDEOGRAPHER: Will the 18 parties please introduce themselves for the 19 record. 20 MR. PRICE: My name is Jeffrey 21 Price. I represent the patent owner in this 22 case, Centripetal Networks, Inc., and I am 23 joined by Jenna Fuller, also of Kramer Levin, 24 and Craig Kronenthal, Banner Witcoff. 25 MR. MCKEOWN: Scott McKeown of	Page 7 1 Q. And how many times have you been 2 deposed as an expert in a patent matter? 3 A. 15 to 20 is the answer. 4 Q. Okay. And have you ever been deposed 5 in an inter partes review proceeding before? 6 A. Yes, I have. 7 Q. And how many times? 8 A. Probably maybe ten, eight or ten. 9 Q. So you know the drill. I'm going to 10 be asking you a series of questions today. I'm 11 going to need your truthful testimony. Will 12 that be a problem? 13 A. Not at all. 14 Q. Okay. Just so we get the record as 15 clear as possible, as you know, it's sometimes 16 difficult when we're doing these things 17 virtually to make sure that we're not talking 18 over each other, but I'm going to do my best 19 today to let you give your full, complete 20 answers to my questions, and I just ask that you 21 extend the same courtesy to me and just let me 22 finish my questions before you answer. Does 23 that sound good? 24 A. Sounds good. 25 Q. Dr. Weissman, can you tell me what you
Page 6 1 Ropes & Gray representing Palo Alto Networks, 2 joined today by Keyna Chow and Andrew Radsch, 3 also of Ropes & Gray. 4 THE VIDEOGRAPHER: Madam Court 5 Reporter, can you please swear in the witness? 6 JON B. WEISSMAN, 7 having been first duly sworn, 8 was examined and testified as follows: 9 DIRECT EXAMINATION 10 BY MR. PRICE: 11 Q. Good morning, Dr. Weissman. How are 12 you today? 13 A. Good morning. Thank you. 14 Q. Are you well? 15 A. I am well. 16 Q. Dr. Weissman, have you ever been 17 deposed before? 18 A. Yes, I have. 19 Q. Roughly, how many times have you been 20 deposed? 21 A. Somewhere between 15 and 20, I would 22 guess. 23 Q. Have you ever been deposed as an 24 expert in a patent matter before? 25 A. Yes, I have.	Page 8 1 did to prepare for your testimony this morning? 2 A. I reviewed my declaration. Reviewed 3 the prior arts, the '856 patent, and had two 4 meetings with Ropes & Gray counsel. 5 Q. Who did you meet with at Ropes & Gray? 6 A. Principally Keyna Chow. But one call 7 was also to Andrew Radsch and another to Scott 8 McKeown. 9 Q. Dr. Weissman, did you write your 10 declaration that you submitted in this case? 11 A. Yes, I did, with assistance from 12 counsel. 13 Q. What do you mean by with assistance 14 from counsel? 15 A. There were drafts that were 16 circulated, you know. Possibly a word or two 17 was changed here and there. I was given the 18 legal language to insert, but the opinions are 19 mine and the declaration is mine. 20 Q. Did you have any input on which claims 21 of U.S. Patent No. 9,917,856, which I'll refer 22 to as the '856 patent today, were challenged in 23 this case? 24 A. I did not. 25 Q. So you were asked by counsel to

Page 9 1 provide opinion on patentability of Claims 124 2 and 25; is that correct? 3 A. That's correct. 4 Q. Do you have any understanding of why 5 those were the only claims that you were asked 6 to provide an opinion on? 7 A. I do not. 8 Q. In the course of your work in 9 providing your opinions about the patentability 10 of Claims 124 and 25, did you have occasion to 11 review any of the other claims of the '856 12 patent? 13 A. I took a look at the full patents, 14 including the claims, but I wouldn't say I did 15 any sort of deep review. 16 Q. And that was because you were not 17 asked to provide an opinion on the patentability 18 of any other claim, of the '856 patent? 19 A. Yes, that's correct. 20 Q. So you never considered whether or not 21 any of the part that was cited in this case 22 rendered any of the other claims of the '856 23 patent obvious? 24 A. I have no opinion. I just didn't do 25 that analysis.	Page 11 1 Q. Are you aware of whether or not the 2 '856 patent has been asserted against Palo Alto 3 Networks? 4 MR. MCKEOWN: Objection; form. 5 THE WITNESS: I am not aware. 6 BY MR. PRICE: 7 Q. Did you review patent owner's 8 preliminary response filed in this case? 9 A. I did take a look at it, yes. 10 Q. Okay. And that preliminary response 11 didn't give you any understanding of whether or 12 not the '856 patent was asserted against Palo 13 Alto Networks? 14 A. Sitting here, I don't recall the 15 details of that. I focused on my documents 16 principally, but I did see it. 17 Q. You skipped -- 18 A. No, I didn't skip it, but I don't 19 remember all the details of it, and you can 20 bring it up and we can look at it if you'd like. 21 Q. I'm sorry, did you say skim or skip -- 22 A. I read it. 23 Q. I'm sorry. I just want to make the 24 record clear. There was a word that you used, 25 and I'm not sure if you said skip or skim?
Page 10 1 Q. Given your rather extensive history as 2 working as an expert on patent matters, did you 3 find it at all odd that you were only asked to 4 provide opinions on a subset of the claims of 5 the '856 patent? 6 MR. MCKEOWN: Objection; form. 7 THE WITNESS: I did not. In IPRs 8 I often am provided a subset of claims and even 9 in litigation. 10 BY MR. PRICE: 11 Q. So in a litigation, you likely 12 understand that there is a set of claims that 13 are asserted against -- by a patent owner 14 against a defendant; is that your understanding? 15 A. In a patent litigation, yes. 16 Infringement litigations. 17 Q. And so in that case, have you ever 18 provided an opinion on fewer than the number of 19 claims that have been asserted against the 20 defendant? 21 MR. MCKEOWN: Objection; scope. 22 THE WITNESS: Sitting here, as I 23 said, I believe I have, though I'm not 24 completely certain. 25 BY MR. PRICE:	Page 12 1 A. I may have said skim, but I read it. 2 Q. In preparing your opinions on the 3 patentability of Claims 124 and 25 of the '856 4 patent, did you discern any major differences 5 between those three independent claims? 6 MR. MCKEOWN: Objection; form. 7 THE WITNESS: I didn't discern 8 any major differences, no. 9 BY MR. PRICE: 10 Q. You are familiar with the 11 Buruganahalli reference; correct? 12 A. That's correct. 13 Q. And for the record, that was a 14 document that was marked as Exhibit 1004 in this 15 proceeding; is that your understanding? 16 A. I honestly don't remember the exhibit 17 numbers. 18 Q. Before we go on, do you have copies of 19 any documents in front of you today? 20 A. I have clean copies of several 21 documents. 22 Q. Can you tell me which documents you 23 have in front of you today? 24 A. Sure. I have a declaration on the 25 '856 patent.

Page 13 1 Q. And that's Exhibit -- we'll just go 2 through them one at a time, if you don't mind. 3 That's Exhibit 1002? 4 A. I also have a copy, clean copy of the 5 '856 patent. 6 Q. Sorry, your declaration is 7 Exhibit 1003; correct? 8 A. As I said, I don't remember. 9 Q. Are the numbers marked on your copies, 10 on the front page? 11 A. Oh, you're right, they are. Sorry, 12 didn't notice that. Correct, it is 1003. 13 Q. Okay, thank you. Then let's move on. 14 What's the next document you have in front of 15 you? 16 A. The '856 patent. 17 Q. Is that Exhibit 1001? 18 A. It is. 19 Q. And what do you have next? 20 A. I have the -- what we're calling the 21 Buru patent. 22 Q. I'm fine with calling it the Buru 23 patent today. That's Exhibit 1004? 24 A. Yes. 25 Q. Okay, what else?	Page 15 1 the declaration. Presumably at the outset of 2 working on this. 3 Q. Do you recall what date you were first 4 engaged to work on this case? 5 A. I don't recall. 6 Q. Do you have a general idea of the time 7 frame? 8 A. I honestly can't recall. I work on a 9 lot of things. I know the date of the 10 declaration. 11 Q. What's the date of the declaration? 12 A. I believe that's November. Let me 13 just confirm that for you. November 18th of 14 2021. 15 Q. What did you refer to, to refresh your 16 memory about the date that your declaration was 17 filed? 18 A. A clean copy of the version. 19 Q. You referred to Page 110 of the 20 declaration? 21 A. Yes, it was on Page 110. 22 Q. That's your signature on Page 110? 23 A. Yes, it is. 24 Q. So this document was executed on 25 November 18th. Do you recall roughly how long
Page 14 1 A. The final document I have is the Baehr 2 patent, that's '231. 3 Q. The '231 patent, that's Exhibit 1005? 4 A. Correct. 5 Q. You don't have any other documents in 6 front of you today? 7 A. I do not. 8 Q. Are those documents clean? And what I 9 mean by clean is they don't have any notes, 10 annotations, highlighting, markings of any kind? 11 A. They are completely clean, printed and 12 not touched. 13 Q. Okay, very good. I have no objection 14 to you referring to hard copies of your 15 documents today. If we discuss anything else, 16 I'll have the document uploaded into the chat. 17 I will likely have the documents put into the 18 chat anyway so that anybody on the line who 19 doesn't have copies in front of them will be 20 able to access them so we're all on the same 21 page. Sound good? 22 A. Sounds good. 23 Q. At what point did you become aware of 24 the Buru patent? 25 A. Sometime prior to the completion of	Page 16 1 before that you were engaged in this matter? 2 A. I do not. It was several months, but 3 I don't remember the exact date. 4 Q. So could have been -- would you say it 5 was prior to June of 2021? 6 A. I would have to check my records. I'm 7 not certain. I'm happy to do that, if you'd 8 like. 9 Q. We may ask for some discovery, just to 10 confirm the date, since it appears that you have 11 documentation that would tell me. But for now, 12 we can move on. 13 Was the Buru patent provided to you, 14 or did you locate the Buru patent yourself? 15 A. I don't recall if during the 16 preparation of the declaration I was just given 17 the patent number, or I got it myself from 18 Internet, or whether it was provided to me in an 19 attachment or something. 20 Q. So when you were approached to work on 21 this matter, you don't recall what materials 22 were sent to you at that time? 23 A. I don't recall what was sent to me 24 versus what I was given or pointed to. 25 Q. Did you perform your own search for

Page 17 1 art that was relevant to the '856 patent? 2 A. I did not. 3 Q. So is it safe to presume that the Buru 4 patent was provided to you? 5 A. As I said, it was provided either as a 6 pointer, given a patent number, or directly 7 given as the patent itself. 8 Q. Okay, I understand. 9 A. Let me actually re-answer the question 10 of whether I did a search. Let me say that I'm 11 not certain. I may have searched for prior art 12 that I'm not certain right now. 13 Q. The same question about the Baehr 14 reference. Was the Baehr reference, which is 15 Exhibit 1005, was that provided to you either as 16 the full patent or, as you refer to it, as a 17 pointer, maybe given the patent number? 18 A. Yes, it was provided to me. 19 Q. And was that provided in conjunction 20 with the '856 patent itself? 21 A. I don't remember if it was provided in 22 the same communications in temporal time frame 23 or if it came later or not. 24 Q. Prior to working on this case, did you 25 have any knowledge of the Buru patent?	Page 19 1 for basically capturing of the packets and 2 processing those for potential threats. 3 Q. Did any of that work involve 4 processing captured encrypted packets for 5 potential threats? 6 MR. MCKEOWN: Objection; form. 7 THE WITNESS: It may have. I 8 don't recall if some of the packets in the logs 9 that we had were encrypted or not. 10 BY MR. PRICE: 11 Q. I mean, did you develop any techniques 12 for developing -- I'm sorry, did you develop any 13 techniques for processing encrypted packets for 14 potential threats? 15 MR. MCKEOWN: Objection; form. 16 THE WITNESS: As I said, there 17 may have been encrypted packets. The technique 18 was to look at signatures of flow IDs, and I 19 believe there was some content analysis. It's 20 been a number of years. So for flow IDs, you 21 obviously can do that with encrypted packets. 22 Sitting here, I can't recall if there were some 23 of those in what we looked at. 24 BY MR. PRICE: 25 Q. Can you explain to me what you mean by
Page 18 1 A. I did not. 2 Q. Do you know or have you had any 3 interactions with either of the inventors listed 4 on the face of the Buru patent? 5 A. No, I have not. 6 Q. And do you have any understanding of 7 where counsel came across the Buru patent? 8 MR. MCKEOWN: Objection; form. 9 THE WITNESS: I have no 10 recollection of that. I believe I was just, 11 like I said, given the patent or pointer to the 12 patent. 13 BY MR. PRICE: 14 Q. I'd like to turn to your declaration, 15 Page 3 and Paragraph 7, in particular. 16 A. Okay. 17 Q. So in Paragraph 7 you state that your 18 work has included packet analysis for network 19 intrusion. Do you see that? 20 A. I do. 21 Q. What is your experience with packet 22 analysis for network intrusion? 23 A. I worked with -- I had a joint NSF 24 grant with data mining and network security 25 faculty, and I built some of the infrastructure	Page 20 1 flow IDs? 2 A. Flow ID is generally the -- an 3 indication of a communication session, and so 4 it's often -- can be represented by destinations 5 and source, IP addresses and port numbers, and 6 sometimes protocol. 7 Q. So if you receive a -- one packet that 8 has a source IP address, a source port, 9 destination IP address, destination port, you 10 might be able to tell that a second packet is 11 part of the same flow if they have the same 12 information in the packet header? 13 MR. MCKEOWN: Objection; form. 14 COURT REPORTER: (Requests 15 clarification.) 16 THE WITNESS: That's correct. 17 BY MR. PRICE: 18 Q. Is that the typical way that a flow 19 analysis is conducted? 20 MR. MCKEOWN: Objection; form. 21 THE WITNESS: I'm not certain 22 it's the typical way. It's a very common way. 23 So I would say it is fairly typical. 24 BY MR. PRICE: 25 Q. And I guess we can jump there. The

Page 21 1 Buru patent discusses flow analysis; correct? 2 A. I do believe it talks about flows, 3 yes. 4 Q. All right. 5 MR. PRICE: Can we have the Buru 6 patent and the declaration, so those are 7 Exhibits 1003 and 1004, uploaded to the chat so 8 everyone here is on the same page? 9 THE VIDEOGRAPHER: Which one is 10 the Buru patent? 11 MR. PRICE: That's Exhibit 1004. 12 THE VIDEOGRAPHER: Thank you. 13 They're both uploaded to the chat. 14 BY MR. PRICE: 15 Q. So if we turn to Column 9 of the Buru 16 patent. 17 A. Okay. 18 Q. Beginning at Line 25, there's a 19 discussion of an IP address and port engine. Do 20 you see that? 21 A. I do. 22 Q. And do you agree that this passage 23 here describes a way to determine what flow a 24 particular packet belongs to? 25 A. Yes, it's describing monitoring of the	Page 23 1 extracting destination domains. So the order in 2 which things are done is not completely clear. 3 One could be done before the other or the 4 opposite. It's not completely spelled out. 5 Q. Can you point me to where you're 6 referring to here? 7 A. Column 10, Lines -- I guess starting 8 at the new paragraph, 37, I guess. 9 Q. I'm sorry, Column 10, Line 37? 10 A. Line 37, at least through 39. 11 Q. So this is a description of -- summary 12 of the block diagram of Figure 2, right? 13 A. Correct. 14 Q. Does this say anything about when the 15 destination domain extraction occurs? 16 A. It does not, nor does the passage you 17 had me read earlier about Figure 1. 18 Q. So we can go back to Figure 1, because 19 there is some explanation of the host name 20 extraction. So starting around Line 44 of 21 Column 9, do you see where it says that: As 22 also shown in Figure 1, a known protocol decoder 23 engine 112 decodes and analyzes traffic flows 24 using known protocols? 25 A. That's what it says.
Page 22 1 traffic flow. 2 Q. Okay. And so then starting at 3 Line 30, after you determined which packet of -- 4 which flow a packet belongs to, the Buru patent 5 discloses determining whether any policies can 6 be applied based on the IP address and port 7 number; correct? 8 MR. MCKEOWN: Objection; form. 9 THE WITNESS: That's exactly what 10 it says. 11 BY MR. PRICE: 12 Q. So when Buru's network monitoring 13 device receives a packet, the first thing it 14 does is determine which flow the packet belongs 15 to; is that right? 16 A. I'm not certain that's the first 17 thing, and of course, what we're looking at may 18 well be one embodiment of Buru. 19 Q. Can you point me to any place in Buru 20 that would disclose something else happening 21 before the network device determines either 22 whether it's a new flow or the packet is part of 23 an old flow? 24 A. Well, other places, for example, 25 there's discussion in Column 10 that talks about	Page 24 1 Q. And a little bit further down it 2 discusses a protocol decoder engine decoding 3 techniques on certain protocols to provide 4 destination domain extraction? 5 A. That's what it says. 6 Q. So if this is happening on an analyzed 7 traffic flow, do you agree that this occurs 8 after the packet is determined to be part of a 9 particular flow? 10 A. It doesn't clearly say we first 11 establish a flow, then we do this domain 12 extraction. I don't -- in my reading of it, I 13 don't think it's completely clear. 14 Q. So when it says that a known protocol 15 decoder engine decodes and analyzes traffic 16 flows, you don't agree that that means that the 17 flow is recognized before it's analyzed? 18 A. It could be referring to or analyzing 19 packets. We will determine if there is protocol 20 flow certainly at some point. It could be the 21 first packet they ever see, right, so the order 22 of when things are done is not completely clear. 23 Q. What does Buru teach about flow 24 analysis for the first packet received in a 25 session?

Page 25 1 A. I'm not seeing or recalling if there's 2 one embodiment or several embodiments for what 3 is the first thing that happens. You can point 4 me to those; I can discuss them. 5 Q. One place we can go to is Column 4, 6 starting at Line 23. 7 A. Yeah, I think we discussed this 8 earlier that it's not completely clear, as I 9 look at this, that, you know, a new flow in 10 terms of as far as a device recognizing this and 11 establishing this as a flow, then it does domain 12 extraction. It obviously recognizes it as a 13 flow at some point, or this will be a flow, part 14 of a flow. It's not clear that that step is 15 happening exactly then and there. 16 Q. Can we turn to Figure 1 itself. So 17 Figure 1 starts at Step 102. Do you see that? 18 A. Yes, I do. 19 Q. And then it proceeds to the check IP 20 port box at 104, which was what we discussed 21 earlier, which was the flow identification; 22 correct? 23 A. As we were talking about in 24 Paragraph 4, what it says about -- 104, in 25 Column 9, it says: Port engine determines an IP	Page 27 1 BY MR. PRICE: 2 Q. What else does it say? 3 A. Based on which policies and set of 4 actions that can be applied to the flow. 5 Q. Okay. Do you agree that the policies 6 and set of actions that are applied to a flow 7 are chosen based on which flow the particular 8 packet is a part of? 9 A. You said policies and actions. 10 Q. Right. So I'm just reiterating what 11 Buru is saying. So it says which policies and 12 set of actions that can be applied to the flow. 13 A. Knowing a packet is connected, 14 correlated to a particular domain, is important 15 to performing security functions. 16 Q. That wasn't my question. My question 17 was about essentially whether or not which flow 18 a packet belongs to determines which policies 19 and set of actions are applied to the flow. 20 A. I would agree, but I would also say 21 that it is also part of the policy to check that 22 this packet corresponds to a particular domain 23 that has been seen, and that that is also part 24 of the rules. 25 Q. So in your answer you said: I would
Page 26 1 address and port number for a monitored flow. 2 Again, I think one could read that as the flow 3 could be determined sort of as we're doing -- 4 subsequent to looking at, say, the domain name. 5 Q. Is the order in which that occurs, 6 whether or not the domain name is extracted or 7 the flow is determined, at all relevant to your 8 patentability analysis, in your opinion? 9 A. I don't believe it is. 10 Q. Can we return to Column 4, the passage 11 that we were talking about, starting on Line 23. 12 This passage refers to extracting information 13 about the destination domain for any given new 14 flow as early as possible. Do you see that? 15 A. I do, and that is some evidence that 16 it was maybe happening before the flow was 17 identified, as early as possible, so -- 18 Q. Why does Buru expose that it's 19 beneficial to extract information about the 20 destination domain as early as possible? 21 MR. MCKEOWN: Objection; form. 22 THE WITNESS: It goes on to say 23 in Paragraph 4: Information about the 24 destination domain can be critical and relevant 25 for security processing.	Page 28 1 also say that it is part of the policy to check 2 that the packet corresponds to a particular 3 domain. What policy are you referring to in 4 that answer? 5 A. When an encrypted packet is received, 6 Buru -- policy that sees whether this packet is 7 correlated with a blacklisted domain name that 8 has been seen earlier. 9 Q. So your answer was referring to the 10 blacklist policy referred to in Buru? 11 A. Well, policy is a broad term. There's 12 a number of different things under that 13 umbrella. So, one is, is something on a 14 blacklist or not. Another aspect of the policy 15 is to check whether encrypted packets are 16 associated with that particular blacklisted 17 domain, a blacklisted domain. 18 Q. How does Buru check whether encrypted 19 packets are associated with a particular 20 blacklisted domain? 21 A. Buru built a table to make that 22 association. 23 Q. Where is that table discussed in Buru? 24 A. Would you mind if I do PDF search? 25 Q. I don't mind. That will make

Page 29 1 everybody's life a lot easier, I think. 2 A. Yeah, I just do not have that at my 3 fingertips. And that's the only thing that's 4 open on this machine is the PDF -- 5 Q. Please feel free to search. 6 A. Okay, thank you. 7 Q. To be clear, please feel free to 8 search through the documents that we discussed 9 that you have in front of you. 10 A. I'm only looking through Buru right 11 now. 12 Q. Okay. Yep, go ahead. 13 A. That table is described in Column 13, 14 I guess Lines 60 to 65 or so. 15 Q. So this table that you're referring 16 to, this portion of the Buru patent, associates 17 host names and identifiers with the policies 18 that are associated with those IP addresses and 19 identifiers? 20 A. Well, as I said, the policy is a broad 21 term, so policy consists of packet filtering 22 rules. So there's rules at different levels. 23 So, you know, one rule is to check it as 24 blacklisted. Another rule is to look in this 25 table and establish a -- see if there's a	Page 31 1 packet is not blacklisted, it's not on the 2 table. We have to check the table to know it's 3 not in the table. 4 Q. Okay. So if a packet is received and 5 it's determined to be part of a blacklisted 6 flow, this table tells you which policy to apply 7 to that packet? 8 A. Well, the determination that the 9 packet is blacklisted is by virtue of its 10 appearance in this table. So you don't know 11 it's blacklisted -- if it's an encrypted packet, 12 you don't know it's blacklisted until you 13 consult the table. So that's the rule to do 14 that. 15 Q. You keep saying that's the rule. What 16 do you mean when you say, so that's the rule to 17 do that? 18 A. Checking the table with respect to 19 that packet. Is that packet represented in this 20 table? Is it associated with a blacklisted 21 domain? 22 Q. And then once that association is 23 made, this table tells you which policy to apply 24 to that packet? 25 A. The way I would say it is Buru has
Page 30 1 correlation. 2 Q. Okay. So am I right to summarize this 3 section of Buru to say that each flow that's 4 recognized at Buru's device is associated in 5 this table with a particular policy? 6 A. I mean, I would say that essentially 7 the rules apply to all the packets in a flow. 8 So I think it's applying the rules on a packet 9 basis. 10 Q. And so this table tells you which 11 rules to apply to packets in any given flow; 12 correct? 13 A. I'm not sure I would characterize it 14 as this table tells you, which the rule is to 15 check this table to determine whether the packet 16 is -- correlates to a domain name that's 17 blacklisted. They're meaning it's in the table, 18 is my reading of this, and then whatever actions 19 are appropriate. 20 Q. Does this table only associate flows 21 with policies when they're blacklisted? 22 A. Again, I would say that the policies 23 are applying to packets in the flow, and I would 24 say no, because the table is still going to be 25 checked, and it's possible that a particular	Page 32 1 implemented rules, one of which is to consult 2 this table for packet, and then take an 3 appropriate action based on what that look-up in 4 the table determined. 5 Q. And so the -- 6 A. The totality of that is part of the 7 policy, it's rules. 8 Q. And one of the appropriate actions 9 would be to apply the policy that's referred to 10 in the table; correct? 11 A. You're not applying a policy. 12 You're -- Buru is executing a set of rules that 13 collectively -- on packets that collectively 14 represent the policy. So the actions, for 15 example, that are taken when a packet is 16 determined to correlate to a domain through this 17 table, there's -- what to do is not specified in 18 this table directly, right. Buru has described 19 what it does in that case. So I just want to 20 make that clear, that the policies and set of 21 rules, not everything is completely specified in 22 the table. 23 Q. Right. But which policy would be 24 applied to a packet matching a flow is specified 25 in a table, right? Isn't that the point of the

Page 33 1 table? 2 A. Again, policies are a broad umbrella, 3 and what this table enables is a packet 4 filtering rule to be checked, and then 5 appropriate action taken, and that component is 6 one of the actions -- one of the things that 7 happens as far as the policy. You describe the 8 policy as a set of rules. That's just one of 9 the rules. 10 Q. So can we just turn to Column 15 of 11 Buru quickly, because I just want to make sure 12 we're on the same page when we're talking about 13 what Buru teaches. So can you just start 14 reading around Line 11 and go down to 21 and let 15 me know when you're done. 16 A. Not on the record, just quietly? 17 Q. Just quietly, that's fine. You don't 18 have to read it into the record. 19 A. Now can you repeat the line numbers? 20 Q. Yeah -- you can read the whole 21 paragraph. Why don't you start with Column 15, 22 Lines 4 through 21. 23 A. Okay. I've read it. 24 Q. So here Buru describes applying a 25 policy based on the destination domain, right?	Page 35 1 understand this invention and what that means, a 2 person of ordinary skill would read policy as 3 the collection of those rules. 4 Q. And so you mentioned earlier one of 5 the rules is a rule to consult this table for a 6 new, incoming packet, right? 7 A. That's part of the rule; correct. 8 Q. And how is that rule carried out in 9 Buru? 10 A. When an encrypted packet is received, 11 then this table will be consulted. So -- 12 COURT REPORTER: (Requests 13 clarification.) 14 THE WITNESS: When an encrypted 15 packet is received, Buru runs a rule that will 16 basically look up this packet in the table and 17 make a check whether there's a correlation from 18 this packet, and a domain that is in this table, 19 which means it's blacklisted, or not. 20 BY MR. PRICE: 21 Q. What information is correlated from 22 the encrypted packet to make that determination? 23 MR. MCKEOWN: Objection to form. 24 THE WITNESS: Buru uses the IP 25 address and port.
Page 34 1 A. And by that, Buru means -- well, what 2 I believe a person of ordinary skill would 3 believe Buru is saying is. Applying a policy in 4 this context means check the packet filtering 5 rules that are relevant in this context. 6 Q. Right. Okay. You don't have any 7 issue with the way Buru talks about applying a 8 policy in this passage, right? 9 MR. MCKEOWN: Objection; form. 10 THE WITNESS: Buru is a valid 11 patent, so -- as far as I know. I'm not a 12 patent attorney; I don't draft patents. 13 BY MR. PRICE: 14 Q. So a person of ordinary skill in the 15 art understands what Buru is talking about here 16 when he or she says destination domain 17 extraction for secure protocols further includes 18 applying a policy based on the destination 19 domain, right? 20 A. Right. Person of ordinary skill is a 21 technical person. You know, you have to put 22 meat on the bones of what does policy mean, 23 right. So we're talking about the execution of 24 packet filtering rules, which is certainly a 25 more tangible concept. So in order to	Page 36 1 MR. PRICE: We've been going for 2 about an hour. Is this a good time for a break? 3 THE WITNESS: Sounds fine. 4 THE VIDEOGRAPHER: We are off the 5 record. The time is 10:01 a.m. 6 (10:01-10:18 - Recess taken.) 7 THE VIDEOGRAPHER: Do we have 8 everyone back? 9 MR. PRICE: Yes. 10 MR. MCKEOWN: Yes. 11 THE VIDEOGRAPHER: We are back on 12 the record. The time is 10:18 a.m. 13 BY MR. PRICE: 14 Q. Dr. Weissman, can you please turn to 15 Paragraph 91 of your declaration. 16 A. I'm there. 17 Q. Paragraph 91 provides a discussion of 18 Buru's Figure 3A; correct? 19 A. It does. 20 Q. On Page 55, right under the 21 reproduction of Figure 3A, do you see where you 22 say: A typical firewall can initially just 23 inspect the handshake traffic? 24 A. I do. 25 Q. There's a parenthetical and it says:

Page 37 1 As all of the application data is encrypted. 2 What does that mean? 3 A. What it means -- let me turn to Buru 4 one second. I believe what a person of ordinary 5 skill would understand that to mean is that the 6 packet subsequent to the setup would, in the 7 case of an SSL/TLS session, would be -- have 8 encrypted data. 9 Q. And that encrypted data can't be 10 decrypted in typical firewalls, like firewall 11 304, right? 12 A. One second. In this figure I don't 13 recall Buru referring to a typical firewall, but 14 a firewall that is an invention, and that does 15 contain a decryption engine. 16 Q. So I'm reading from the quote here on 17 Page 55. And your citation here includes the 18 passages from Column 10, 54 to 61, which talk 19 about a typical firewall, and 11, 7 through 42, 20 if that helps you. 21 A. Yeah, I'm not necessarily going to say 22 it's typical, because typical means outside the 23 scope of the patent. It clearly is saying 3A is 24 associated with some embodiments. So I just 25 want to make that clear.	Page 39 1 data so that it can detect firewall and policy 2 rule violations, right? 3 A. Well, as I stated earlier, the 4 firewall can be implemented in a variety of 5 different ways. What's described -- one of the 6 embodiments described here expressly is that 7 there is a component called a decryption engine 8 that the firewall will send certain traffic to, 9 certain encrypted traffic to. 10 Q. So, for example, if a session 11 associated with the destination domain is on a 12 blacklist, encrypted traffic can be sent to that 13 decryption engine so that you can determine 14 whether or not there have been any policy 15 violations? 16 A. To restate, policy is a large umbrella 17 involving a variety of packet filtering rules, 18 and a variety of rules are already in force 19 prior to the potential sending of a packet to 20 the decryption engine. But I would certainly 21 agree that decrypting the packet and examining 22 the content for further potential security 23 threats is certainly part of the policy. 24 Q. So that's basically what's described 25 in Column 7, Lines 39 through 67, for example?
Page 38 1 Q. Is it your understanding that the 2 firewall of Figure 3A performs decryption? 3 A. The firewall utilizes a component 4 called a decryption engine to perform 5 decryption. 6 Q. I just want to make completely sure 7 we're on the same page. You're referring here 8 to the firewall 304 of Figure 3A? Can you point 9 me to where that's decryption. 10 A. I'm sorry, I do see the word typical 11 later. It's also an embodiment. To your 12 question, this firewall also has described 13 subsequent as, for example, packet filtering 14 rules that will cause a split session to be 15 created and packets routed to a decryption 16 engine. 17 Q. Returning to my original question, do 18 you agree that typical firewalls are not able to 19 inspect application data because it's encrypted? 20 We can refer to this portion that you cite here 21 on Column 11 starting around Line 2 to 7. 22 A. Here Buru is stating that firewalls 23 typically cannot decrypt encrypted traffic. 24 Q. Okay. But Buru also discloses an 25 embodiment where the firewall can decrypt the	Page 40 1 A. The firewall is running a packet, 2 filtering rules to make a decision what to do, 3 and one of those rules, one of those decisions, 4 is the need to decrypt this packet, or it needs 5 to be decrypted. 6 Q. Can we turn to Column 6, Line 12. So 7 is this what you mean? Is this what you're 8 referring to, so you can determine whether or 9 not a new session using a secure protocol should 10 be initially allowed based on a policy, and then 11 if the flow is determined to be permissible 12 prior to the setup of the encrypted 13 communication for that flow, the flow can be 14 allowed and the policy may require that the 15 session be decrypted for further analysis? 16 A. And the session or flow, so to speak, 17 is represented as a sequence of packets. So the 18 rules are applied to the packets therein. But 19 so I would say the rules are applied to the 20 packets, but -- the rules collectively calling 21 them a flow, but they are applied on a 22 per-packet basis. 23 Q. And the same policy is applied to each 24 packet in the flow, right? 25 A. Well, each packet, anywhere, is

Page 41 1 subject to a particular rule that, as we 2 described earlier, if it's encrypted, determine 3 correlation. And if it's associated with a 4 blacklisted domain, then the packets will be 5 treated similarly, as far as I understand that. 6 I don't recall another embodiment where 7 encrypted packets that correlate to the same 8 domain are treated differently. It's possible, 9 but I don't recall. 10 Q. Down at the bottom of Page 55 you have 11 this sentence that begins: The firewall then 12 filters unencrypted packets. Do you see that? 13 A. Yes. 14 Q. What does the firewall do with 15 unencrypted packets that corresponds to the 16 filtering that you refer to here? 17 A. So filtering is the application with 18 packet filtering rules. And so unencrypted 19 packets are going to be -- the rule is to take a 20 look at them, and if they're handshake traffic, 21 take a look inside that, and if there is a 22 domain, check to see if that's on a blacklist. 23 Q. And what would happen if the domain 24 for an unencrypted packet is on the blacklist? 25 A. That would be recorded, remembered,	Page 43 1 from Buru, so let me take a quick look. 2 Q. Take your time, please. 3 A. Yeah, so Buru says -- I'll just pick 4 one. It's the same over and over. In 5 Paragraph 7, Lines 39 to, say, all the way to 6 51, it's describing that if the destination 7 domain is on a white list, then subsequent 8 encrypted packets will not be decrypted, but 9 routed to the decryption engine. So presumably 10 passed through. 11 Q. Where are you reading? 12 A. I'll go back there. 13 Q. I'm sorry, 39 to 51? 14 A. Yes, Paragraph 7, 39 to, I guess, 51. 15 And so it's saying what you don't do if it's on 16 a white list. Meaning you do something, but 17 it's different. 18 Q. Let's return to Paragraph 7 of your 19 declaration. 20 A. Yes. 21 Q. So previously I asked you about your 22 prior work in packet analysis for network 23 intrusion. The next item on this list is proxy 24 routing in edge networks. Do you see that? 25 A. I do.
Page 42 1 and one of the ways that's done is in this table 2 I talked about. And other places in Buru where 3 that also is -- that state is remembered. 4 Q. Is that the only thing Buru does with 5 blacklisted unencrypted packets? 6 A. I believe Buru has different 7 embodiments, so sort of essentially different 8 flavors of that rule. It could choose to block 9 the session. And of course, if it's not on the 10 blacklist, it would just allow it through. But 11 if it's on the blacklist, it also -- there's 12 embodiments where it will also decide that it 13 needs to set up some state and allow encrypted 14 packets to come in to do sort of further 15 analysis potentially. 16 Q. If the handshake unencrypted packet is 17 blocked before the session is set up, there 18 wouldn't be any encrypted packets received for 19 that session, right? 20 A. I agree. 21 Q. What does Buru teach to do if it 22 receives an unencrypted handshake packet that it 23 determines to be on a white list? 24 A. I don't want to just give an answer 25 off the cuff. I'd like to use specific language	Page 44 1 Q. Can you describe what proxy routing in 2 edge networks is? 3 A. Sure. So this work was to determine 4 if there was better route between two end points 5 than IP routing would naturally follow. So 6 using intermediate nodes to establish multiple 7 connections so that the routing path might 8 actually be cheaper, might actually be -- and 9 this is a well-known phenomenon. Even if you 10 establish a bunch of connections, transport 11 level connections, you can sometimes outperform 12 IP level routing. So the proxy was set up to 13 try to do that. 14 Q. What is the role of the proxy in this 15 scenario? 16 A. The proxy in this case was an 17 intermediary that would set up these sort of 18 interior connections, split connections, if you 19 want to use that term. So there are a series of 20 proxies, and they would form connections to each 21 other, actually, as a way to route the packet. 22 Q. So is this done in order to determine 23 an optimal path, or would you continue once 24 you've kind of found the best path, to continue 25 using multiple connections between the end

Page 45 1 points? 2 A. Yes, so this approach being an 3 academic project, so, you know, it was what it 4 was. So it built tables of latencies between 5 the nodes in the specific network that we were 6 working in, the specific host that we knew we 7 were communicating with. And it is certainly 8 possible that the IP would be the best and it 9 would then pass it through. If not, it would 10 determine what sets of connections might be 11 preferable to that path and establish those in 12 routing packet. 13 Q. Does the term proxy have a 14 well-understood meaning in the art of computer 15 networking? 16 A. It's a term of art. However, there 17 are a number of different ways in which proxies 18 are used, let's say that. In all cases that I 19 know of, for the common future, it's thought to 20 be sort of an intermediary. 21 Q. What do you mean by intermediary? Can 22 you give me an example of a proxy that acts as 23 an intermediary to kind of eliminate what the 24 term might mean to a person of ordinary skill in 25 the art?	Page 47 1 decryption engine is playing in the 2 communication flow, would reasonably conclude 3 that it's acting as a proxy. 4 Q. What is it about the decryption engine 5 that would lead a person of ordinary skill in 6 the art to understand it as a proxy? 7 A. Well, that it, you know, sits on the 8 path between the sender and receiver in this 9 particular case and it's making a decision. So 10 the end points aren't even aware, potentially, 11 that something is -- they're trying to set up an 12 SSL connection. They're not even aware that 13 there's this component that is decrypting the 14 packet to make further decisions about it. And 15 the packet may be allowed through, but the end 16 points have no idea this happened. But anyway, 17 there's this intermediary, so you have to look 18 at the examples, and I believe a person of 19 ordinary skill would conclude that it is a proxy 20 of the type. 21 Q. Can we turn to Figure 6 of the Buru 22 reference? 23 A. I see it. 24 Q. So am I to understand that this SSL 25 decryption box 610 is what you contend to be a
Page 46 1 A. Yeah there's many, many types of 2 examples. So one that's maybe familiar to 3 people is a web proxy where the client wants to 4 fetch a web page from an origin server, and -- 5 COURT REPORTER: (Requests 6 clarification.) 7 THE WITNESS: A client may want 8 to fetch a web page from an origin server, but 9 that request may be directed to a proxy which 10 might have the web page. So it's sort of -- 11 proxy is kind of -- you know, can sit between 12 different network components and perform very 13 different roles, depending on what the proxy is 14 supposed to do. 15 BY MR. PRICE: 16 Q. Did you apply that meaning of the term 17 proxy as basically intermediary in your analysis 18 of whether or not the challenge of claims of the 19 '856 patent are obvious? 20 A. I didn't construe -- let me just 21 clarify. I didn't construe proxy. Proxy is a 22 proxy, and one has to look at what the role -- 23 what role the intermediary is playing. And so I 24 believe a person of ordinary skill of the 25 patent, understanding the rule that the	Page 48 1 proxy in the Buru reference? 2 A. That's what I believe the person of 3 ordinary skill would conclude. 4 Q. Would a person of ordinary skill in 5 the art understand the entire firewall here to 6 be a proxy, since it sits between the two end 7 points? 8 A. That's an interesting question. You 9 know, it sort of depends. If the firewall is 10 part of a router, it likely would not make that 11 judgment, or one would have to look at that 12 situation. A firewall on its own, possibly. It 13 would depend on the context. You know, I would 14 need to kind of see the network and see the 15 setup and understand who is communicating and 16 that sort of thing. 17 Q. What kind of information would you be 18 looking for to determine whether or not a 19 particular firewall would qualify as a proxy? 20 A. Well, there are different types of 21 proxy functions, and you know, if the firewall 22 was performing functions that you would 23 typically associate with proxy, it's possible 24 you might call it a proxy firewall. That term 25 has been used. But other folks might call it a

Page 49 1 firewall. So proxy is a very kind of broad 2 concept. 3 Q. What about the individual -- other 4 individual boxes here in the data plane? So 5 let's take the flow box for -- which we talked 6 about earlier as an example. Is that flow step 7 or box, for a better word, a proxy, under your 8 understanding of the term? 9 A. Flow 608 is described as merely 10 identifying packets as being part of a larger 11 flow or session. I -- you know, on its face, 12 that is not necessarily a proxy function. If 13 something were done, perhaps if some types of 14 processing or functions were done with those, 15 it's possible one could do it that way. But if 16 it's merely saying -- you know, doing an 17 association, I think a person of ordinary skill 18 would likely not refer to that as a proxy. 19 Q. And how come? 20 A. I'm sorry? 21 Q. How come? 22 A. Associating packets as part of a 23 larger unit is fairly routine conventional 24 function carried out by network devices, 25 firewalls, and other things. I think that,	Page 51 1 component that's doing this. And I would say 2 the function of decryption would qualify to make 3 that component viewable as a proxy. 4 Q. What about some of the other 5 functionality here, like decoding and applying a 6 policy, at boxes 614 and 620? 7 A. I don't think decoder is -- decoder is 8 described as a job is to assemble packets that 9 are out of order, and again, that is something 10 that people understand is performed in the 11 network. Was there another box? 12 Q. Yeah, the policies box, 620. 13 A. As I believe I say in the declaration, 14 numerous places, I believe, that the policies as 15 a whole, there's some here, there's some other 16 places. I mean, policy is sort of an umbrella 17 carried out by the firewall. So I would say 18 they're not, you know, a proxy. This is the 19 kind of basic functionality of the firewall, 20 which utilizes a proxy to carry out certain 21 special functions. 22 Q. So a proxy has to perform special 23 functions that are not typically done by a 24 device that they're happening on? Is that -- 25 A. I'm not construing the term. I'm
Page 50 1 again, it depends what the intermediary is 2 doing, in some sense, as to whether it would 3 qualify as a proxy. So I think in the context 4 of Buru, the 608 box I haven't really given a 5 ton of thought, but just here, I'd say probably 6 not. 7 Q. So what is it that differentiates what 8 happens with the association of the packet to a 9 particular flow or box 608 that makes that not a 10 proxy functionality, whereas the decryption of 11 the packet after it's associated with a flow is 12 a proxy functionality? 13 A. I think one distinction is that proxy 14 function usually carries out a particular -- a 15 typical function that the, in this case, end 16 points may or may not be aware of. Now, 17 associating of packets as being, you know, part 18 of the same session, I think everybody 19 understands that TCP is -- you know, requires 20 that that be done at some point, to do traffic 21 management and things like that. So it's not 22 really a proxy function, it's kind of a key 23 function. 24 Whereas decryption is certainly not 25 something that is done routinely. There's a	Page 52 1 saying one has to look to see what -- it depends 2 what the functions are. By special, I mean not 3 something that the normal network, you know, 4 implementation typically do. 5 Q. So if a typical firewall couldn't 6 check encrypted packets for policy violations, 7 but the firewall of Figure 6 can check encrypted 8 packets for policy violations by decrypting them 9 first, that's not a special functionality 10 performed by this policy box in Figure 6? 11 MR. MCKEOWN: Objection; form. 12 THE WITNESS: Well, the firewall 13 itself doesn't do encryption. It basically 14 tells -- it makes a decision, yes, there needs 15 to be a decryption. It doesn't have that 16 functionality directly, so it applies a policy, 17 a rule, that says -- you know, concludes this 18 needs to be decrypted, then it routes it over to 19 the proxy, or the decryption engine in this 20 case, as an example, to go ahead and do further 21 analysis. 22 And I just want to add, you know, I 23 think you know my position in the declaration, 24 that, you know, it would additionally be obvious 25 to represent the decryption engine as a separate

Page 53 1 component entity that is communicated with the 2 IP-3 level routing. I mean, there's many ways 3 it could be realized, and those would be obvious 4 and there are advantages to doing so. 5 Q. Sure, I understand that. I'm really 6 trying to understand -- 7 A. Yeah, I'm just trying to clarify. 8 Q. You do recognize that this Figure 6 9 refers to element 402, which is the security 10 device, right? I mean, I think your 11 clarification was meant to clarify that you 12 understand that all of these boxes are part of a 13 security device or firewall, but that individual 14 elements of it could also exist outside, is 15 that -- 16 A. My position is I believe the 17 decryption engine, particularly box 610, is a 18 proxy. But if -- but in addition, if it were 19 decided that it wasn't, somehow, it would 20 additionally be obvious to make it a separate 21 component. 22 Q. Why would it be obvious to take the 23 decryption engine outside of the firewall and 24 put it somewhere else? 25 A. Decryption is an expensive operation,	Page 55 1 somebody eavesdropping or somebody getting 2 access to that decrypted packet. So I think it 3 also follows some of Baehr's motivation. 4 Q. Are you aware of whether or not the 5 term proxy system as it's used in the '856 6 patent has been construed before this case was 7 initiated? 8 A. I am not aware. 9 Q. So you were not asked to opine on 10 whether any prior constructions of the term 11 proxy system were consistent with how a person 12 of ordinary skill in the art would construe the 13 term? 14 A. By absence of this discussion, I 15 applied what I presumed to be the plain and 16 ordinary meaning of the term, but I was not 17 offered any other constructions to apply. 18 Q. Are you aware of whether or not the 19 term network-threat indicators has been 20 construed prior to the initiation in this case? 21 A. I'm not aware if it has or not. 22 Q. Can you turn to Paragraph 85 of your 23 declaration? 24 A. Okay. 25 Q. Do you see where you state: I
Page 54 1 and the firewall has to process packets very 2 quickly. So it is under the gun in terms of 3 performance. Performance may be one reason. 4 Another component with its own CPU likely would 5 improve network performance. So that's one 6 reason. 7 Q. You are familiar with the Baehr 8 reference, correct, Exhibit 1005? 9 A. Yes, I am. 10 Q. Does Baehr disclose moving a 11 decryption engine outside of the firewall and 12 into a separate device? 13 A. Baehr describes a number of reasons 14 why using a separate proxy is advantageous. It 15 doesn't give a specific example of a decryption 16 engine but, you know, there's sufficient 17 motivation to sort of -- to look to a reference 18 like this, which has isolated separate proxies, 19 in my view. 20 And I would add, you know, Baehr talks 21 a lot about security benefits in using a proxy, 22 and, you know, given that the decryption engine 23 is using session keys to basically, you know, 24 open up the text, one could easily argue there's 25 a security risk there, potentially, with	Page 56 1 understand the term network-threat indicator has 2 been interpreted to mean indicators that 3 represent the identity of a resource associated 4 with a network threat? 5 A. I do see that. 6 Q. Okay. So does that refresh your 7 recollection about whether or not you were aware 8 of whether that term has been construed prior to 9 the initiation in this case? 10 A. I don't. I mean, I think maybe the 11 wording could be a little bit better. I was 12 provided the construction, and I've applied the 13 construction. So somebody, you know, obviously 14 created the construction, right, and that's what 15 I mean by has been interpreted. I don't know 16 that it was officially used in any other 17 matters. I honestly don't know. 18 Q. But you do use the term, I understand 19 that the term has been interpreted. Are you 20 saying that -- 21 A. Right. That just means that I 22 understand that this is the construction that 23 I'm applying. 24 Q. But you say has been interpreted, 25 which means that it was interpreted this way at

Page 57 1 some point in the past, right? 2 A. Again, I think it's perhaps sloppy 3 language on my part. I don't recall, you know, 4 any discussion that this construction is one 5 that comes from another matter. It may. I 6 don't know. 7 Q. Okay. But you did apply this 8 termination in your analysis, right? 9 A. I did apply this meaning of 10 network-threat indicator in my analysis. 11 Q. Can you show me an example of where 12 you used this interpretation in your analysis? 13 A. Okay, so the meaning is indicators 14 that represent the identity of a resource 15 associated with a network threat. And let me 16 find an example. So in the discussion of Claim 17 180, Claim 180 is where the patent describes 18 that these are the criteria, these are the data 19 that can be used. One of them is, for example, 20 URI/URL, which I do describe how Buru discloses 21 filtering using that, and URI, you know, is an 22 indication of a resource that may be of concern. 23 So that's an example. 24 Q. Where do you find in Buru the idea 25 that a URI is a -- let me make sure I get the --	Page 59 1 the blacklist and so forth in that paragraph. 2 Q. In which paragraph? 3 A. Paragraph 7 -- 4 Q. Column 7? 5 A. Yeah, sorry, I keep saying paragraph. 6 Sorry. Column 7. It describes blacklist, 7 destination domain is on a blacklist, and/or, of 8 course, that could be, you know, interpreted as 9 conjunctive or disjunctive, talking about using 10 URLs as a basis for filtering. So I think the 11 person of ordinary skill could certainly 12 reasonably read that as a network-threat 13 indicator in Buru. 14 Q. Does Buru describe blacklisted 15 destination domains as being associated with 16 network threats? 17 A. So Buru does not expressly use the 18 word threat, except like in claims. But a 19 person of ordinary skill would understand when a 20 domain is -- matches something on a blacklist. 21 A blacklist are things you should be worried 22 about as a potential network threat. 23 Q. So my -- I'm sitting in my office here 24 in New York, and I'm not allowed to visit 25 Facebook on my own computer here. I presume the
Page 58 1 indicator -- indicator that represents the 2 identity of a resource associated with a network 3 threat? 4 A. One place would be Column 7, sort of, 5 I guess, down from, I don't know, 48 to 51, it 6 describes, you know, a URL -- using URL as a 7 basis for a filtering policy. And it's in the 8 context of this discussion about blacklists and 9 concerned resources, identity of concerned 10 resources. So I take it that a person of 11 ordinary skill understands that this refers to 12 that the URL is a network -- could be a 13 network-threat indicator, or is an example of a 14 URI. 15 Q. What do you mean it could be a 16 network-threat indicator? 17 A. Well, I mean, it -- let me get this 18 straight: In the construction, indicators 19 represent the identity of a resource associated 20 with a network threat. So assuming the URLs are 21 good, URIs are good, some are blacklist, some 22 are not good, it's a threat, and it's describing 23 filtering rules. To URLs, URIs, which clearly 24 are a resource, identity of a resource, and it's 25 describing that in the context of other threats,	Page 60 1 way that the network administrator stops me from 2 visiting Facebook is by putting that URL or URI 3 on a blacklist. Would you agree? 4 A. I don't know how it's been implemented 5 there. I don't know. 6 Q. I guess my question is, does the fact 7 that a URL or URI is on a blacklist necessarily 8 mean that that URL or URI has been determined to 9 be associated with a network threat? 10 MR. MCKEOWN: Objection; scope. 11 THE WITNESS: I think if -- in 12 the scope of Buru, because one of the potential 13 actions to take on encrypted packets that might 14 relate to HTTPS sessions or SSL sessions is to 15 decrypt and look for concerning patterns. To 16 me, then, the domain name URI is -- Buru is -- 17 the blacklists in question here are potential 18 network threats. Because it's not necessarily 19 blocking every blacklist. Handshake, all right, 20 some are going through and then we do deeper 21 analysis, there is deeper analysis in some 22 cases. 23 MR. PRICE: We've been going for 24 about another hour. Does another ten-minute 25 break sound good?

Page 61 1 THE WITNESS: Sounds good. 2 THE VIDEOGRAPHER: We are off the 3 record. The time is 11:23 a.m. 4 (11:23-11:35 p.m. - Recess taken.) 5 THE VIDEOGRAPHER: Looks like we 6 have the main team. Are we ready to proceed? 7 MR. PRICE: We are. 8 THE VIDEOGRAPHER: We are back on 9 record. The time is 11:35 a.m. 10 BY MR. PRICE: 11 Q. Welcome back. 12 A. Thank you. 13 Q. I would like now to turn to pages 107, 14 108 of your declaration. 15 A. Okay. 16 Q. Okay. So this section talks about 17 secondary considerations. Do you see that? 18 A. Oh, I'm sorry, I thought you said 19 Paragraph 107. 20 Q. Oh, no, sorry. Starting with 21 Paragraph 159. 22 A. Page 107. Yes, it does. 23 Q. What is your understanding of what 24 secondary considerations refer to? 25 A. My understanding is that in the	Page 63 1 considered is Exhibit 1029? 2 A. Yeah, I will have to say that, I mean, 3 that's probably -- some of these may have been 4 in the petition. I don't recall really 5 examining that particular reference. 6 Q. Was it provided to you? 7 A. I don't recall seeing it. 8 Q. Were any other transcripts of the 9 trial between Centripetal and Cisco provided to 10 you before your preparation or in the midst of 11 preparing your declaration? 12 A. Let me check just to be certain. I 13 don't recall seeing any. 14 Q. Okay. So you're not aware of whether 15 or not Exhibit 1029, or any other transcripts 16 between the trial of Centripetal and Cisco, 17 actually included public information touching on 18 objective indicia of nonobvious; is that 19 correct? 20 MR. MCKEOWN: Objection; form. 21 THE WITNESS: I know nothing 22 about the Cisco matter, and my statement here is 23 in that I have not been provided any -- you 24 know, in my analysis I have not been provided 25 any public information.
Page 62 1 determination of whether invention is obvious to 2 a person of ordinary skill, one may consider 3 certain objective factors that might need to be 4 weighed in that decision. 5 Q. Okay. Paragraph 159, you state: I 6 understand that the underlying evidence is not 7 publicly available, about evidence of secondary 8 considerations the patent owner presented in 9 previous litigation. 10 Do you see that? 11 A. It's mentioning the previous 12 litigation. It's also mentioning, which I'm 13 aware of to a certain extent, in that the 14 underlying evidence is not publicly available. 15 I think I'm referring to in this matter, but 16 anyway. 17 Q. To what extent are you aware of the 18 prior litigation involving Cisco? 19 A. I know there was prior litigation. I 20 don't know the details of that, and I was 21 informed that, you know, the issue of secondary 22 considerations arose with respect to '856 in 23 that matter, so I was made aware of that. 24 Q. Okay. Do you see there was one of the 25 exhibits that you list in your list of materials	Page 64 1 BY MR. PRICE: 2 Q. Okay. In Paragraph 160 you state: To 3 the extent patent owner alleges secondary 4 considerations in this proceeding, it is my 5 opinion that they would not outweigh the strong 6 evidence of obviousness of the '856 patent 7 claims. 8 Do you see that? 9 A. I do. 10 Q. How were you able to make that 11 determination without having seen or been aware 12 of the information that exists in the public 13 record or information that patent owner might 14 provide in the future? 15 A. In my opinion the obviousness is clear 16 and convincing; it's extremely persuasive to me. 17 I think it's extremely strong, and I believe one 18 of the -- you know, it's possible that even in 19 the presence of some secondary considerations 20 the strength of the obvious argument can weigh 21 strong -- can weigh -- tilt toward that it is 22 invalid. And that's my current feeling. But 23 you're right, I don't know the public 24 information, but I think the obviousness in this 25 case is quite strong.

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	Page 65 Q. Okay. So is it your position that no possible evidence of secondary considerations would change your analysis in this case? A. I wouldn't make such a blanket statement. I would have to analyze the secondary considerations. But I will say this general area of network security is an ongoing problem and people are continually working on it. MR. PRICE: I don't have any further questions today. Thank you for your time. THE WITNESS: Thank you. MR. MCKEOWN: We're done. COURT REPORTER: (Requests orders for the record.) MR. MCKEOWN: No, not necessary. MR. PRICE: Standing order. THE VIDEOGRAPHER: This concludes today's deposition. The time is 11:44 a.m. (11:44 a.m. - Adjournment.) ** ** *	

1	C E R T I F I C A T E
2	STATE OF NEBRASKA)
3	COUNTY OF DOUGLAS) Ss.
4	I, Cheryl A. Rooney, Registered
5	Professional Reporter, General Notary Public
6	within and for the State of Nebraska, do hereby
7	certify that the foregoing testimony of JON B.
8	WEISSMAN was taken by me in shorthand and
9	thereafter reduced to typewriting by use of
10	Computer-Aided Transcription, and the foregoing
11	sixty-six (66) pages contain a full, true and
12	correct transcription of all the testimony of
13	said witness, to the best of my ability;
14	That I am not a kin or in any way
15	associated with any of the parties to said cause
16	of action, or their counsel, and that I am not
17	interested in the event thereof.
18	IN WITNESS WHEREOF, I hereunto affix
19	my signature and seal this 24th of August, 2022.
20	
21	_____
22	CHERYL A. ROONEY, RPR
23	GENERAL NOTARY PUBLIC
24	Registered Professional Reporter
25	My Commission Expires: November 24, 2022

<u>WORD INDEX</u>			
< 1 >	1900 2:13	463-5000 3:17	11:2, 12 12:3, 25
1 4:2 23:17, 18,	< 2 >	48 58:5	13:5, 16 17:1, 20
22 25:16, 17	2 4:2 23:12	< 5 >	46:19 55:5 62:22
10 4:16 22:25	38:21	508-4600 2:8	64:6
23:7, 9 37:18	2:18-cv-00094	51 43:6, 13, 14	< 9 >
10:01 36:5	4:15	58:5	9 21:15 23:21
10:01-10:18 36:6	20 6:21 7:3	54 37:18	25:25
10:18 36:12	20006-6807 2:8	548 4:15	9,917,856 1:4
1001 4:8 13:17	202 2:8	55 36:20 37:17	8:21
1002 13:3	2020 4:16	41:10	9:01 1:17 5:10
1003 4:8 13:7, 12	2021 15:14 16:5	< 6 >	91 36:15, 17
21:7	2022 1:17 5:9	6 40:6 47:21	94065 3:11
10036 3:6	66:19, 24	52:7, 10 53:8	94303-2284 2:14
1004 4:8 12:14	2099 2:7	60 29:14	< A >
13:23 21:7, 11	21 33:14, 22	60606 3:17	a.m 5:10 36:5, 12
1005 4:8 14:3	212 3:6	608 49:9 50:4, 9	61:3, 9 65:20, 21
17:15 54:8	23 25:6 26:11	61 37:18	ability 66:13
102 25:17	231 4:8 14:2, 3	610 47:25 53:17	able 14:20 20:10
1029 4:8 63:1, 15	24 66:24	614 51:6	38:18 64:10
104 25:20, 24	24th 66:19	617-4000 2:14	about 9:9 15:16
107 61:13, 19, 22	25 9:2, 10 12:3	620 51:6, 12	17:13 21:2 22:25
108 61:14	21:18	63 4:16	23:14, 17 24:23
11 33:14 37:19	< 3 >	65 29:14	25:23, 24 26:11,
38:21	3 4:3 18:15	650 2:14 3:12	13, 19, 23 27:17
11:23 61:3	30 22:3	66 4:4 66:11	33:12 34:7, 15, 23
11:23-11:35 61:4	304 37:11 38:8	67 39:25	36:2 37:19 42:2
11:35 61:9	312 3:17	68102 3:23	43:21 47:4, 14
11:44 65:20, 21	333 3:10	6th 2:13	49:3, 6 51:4
110 15:19, 21, 22	3600 3:16	< 7 >	54:21 56:7 58:8
112 23:23	37 23:8, 9, 10	7 18:15, 17 37:19	59:9, 22 60:24
1177 3:5	39 23:10 39:25	38:21 39:25 43:5,	61:16 62:7 63:22
12 40:6	43:5, 13, 14	14, 18 58:4 59:3,	absence 55:14
124 9:1, 10 12:3	3A 36:18, 21	4, 6	academic 45:3
13 4:8 29:13	37:23 38:2, 8	700 3:11	access 14:20 55:2
1321 3:22	< 4 >	71 3:16	acting 47:3
14 4:8	4 4:3, 4 25:5, 24	715-9100 3:6	action 32:3 33:5
15 6:21 7:3	26:10, 23 33:22	752-1728 3:12	66:16
33:10, 21	402 53:9	795 4:8	actions 27:4, 6, 9,
159 61:21 62:5	402)556-2037 3:23	< 8 >	12, 19 30:18 32:8,
160 64:2	402)556-5000 3:23	85 55:22	14 33:6 60:13
180 57:17	42 37:19	856 4:8 8:3, 22	acts 45:22
18th 15:13, 25	44 23:20	9:11, 18, 22 10:5	add 52:22 54:20
19 1:17 5:9			addition 53:18

additionally 52:24 53:20 address 20:8, 9 21:19 22:6 26:1 35:25 addresses 20:5 29:18 Adjournment 65:21 administrator 60:1 advantageous 54:14 advantages 53:4 affix 66:18 after 22:3 24:8 50:11 Again 26:2 30:22 33:2 50:1 51:9 57:2 against 10:13, 14, 19 11:2, 12 agree 5:13 21:22 24:7, 16 27:5, 20 38:18 39:21 42:20 60:3 ahead 29:12 52:20 alleges 64:3 allow 42:10, 13 allowed 40:10, 14 47:15 59:24 already 39:18 ALTO 1:3 2:14 6:1 11:2, 13 Americas 3:5 analysis 9:25 18:18, 22 19:19 20:19 21:1 24:24 26:8 40:15 42:15 43:22 46:17 52:21 57:8, 10, 12 60:21 63:24 65:3 analyze 65:5 analyzed 24:6, 17	analyzes 23:23 24:15 analyzing 24:18 and/or 59:7 ANDREW 2:8 6:2 8:7 andrew.radsch@ro pesgray.com 2:14 annotations 14:10 another 8:7 28:14 29:24 41:6 51:11 54:4 57:5 60:24 answer 7:3, 22 27:25 28:4, 9 42:24 answers 7:20 any 8:20 9:4, 11, 15, 18, 21, 22 11:11 12:4, 8, 19 14:5, 9, 10 17:25 18:2, 6 19:3, 11, 12 22:5, 19 26:13 30:11 34:6 39:14 42:18 55:10, 17 56:16 57:4 63:8, 13, 15, 23, 25 65:10 66:14, 15 anybody 14:18 anything 14:15 23:14 anyway 14:18 47:16 62:16 anywhere 40:25 APPEAL 1:2 appearance 31:10 APPEARANCES 2:1 3:1 4:2 Appearing 2:2, 5 3:3, 21 5:12 appears 16:10 application 37:1 38:19 41:17 applied 22:6 27:4, 6, 12, 19 32:24 40:18, 19,	21, 23 55:15 56:12 applies 52:16 apply 30:7, 11 31:6, 23 32:9 46:16 55:17 57:7, 9 applying 30:8, 23 32:11 33:24 34:3, 7, 18 51:5 56:23 approach 45:2 approached 16:20 appropriate 30:19 32:3, 8 33:5 approximate 5:10 are 5:4 6:11, 14 8:18 10:13 11:1 12:10 13:9, 11 14:8, 11 21:6 23:2 24:22 27:6, 7, 19 28:3, 15, 19 29:18 30:19, 23 32:15 33:2 34:5 36:4, 11 38:18 39:18 40:18, 19, 21 41:8, 19 43:11 44:19 45:17, 18 46:19 48:20 51:9, 23 52:2 53:4, 12 54:7 55:4, 18 56:19 57:18 58:20, 21, 22, 24 59:21 60:17, 20 61:2, 6, 7, 8 62:17 65:8 area 65:7 aren't 47:10 argue 54:24 argument 64:20 arose 62:22 art 17:1, 11 34:15 45:14, 16, 25 47:6 48:5 55:12 arts 8:3	asked 8:25 9:5, 17 10:3 43:21 55:9 asking 7:10 aspect 28:14 assemble 51:8 asserted 10:13, 19 11:2, 12 assistance 8:11, 13 associate 30:20 48:23 associated 28:16, 19 29:18 30:4 31:20 37:24 39:11 41:3 50:11 56:3 57:15 58:2, 19 59:15 60:9 66:15 associates 29:16 Associating 49:22 50:17 association 28:22 31:22 49:17 50:8 assuming 58:20 attachment 16:19 attorney 34:12 August 1:17 5:9 66:19 available 62:7, 14 Avenue 2:7, 13 3:5 aware 11:1, 5 14:23 47:10, 12 50:16 55:4, 8, 18, 21 56:7 62:13, 17, 23 63:14 64:11 < B > back 23:18 36:8, 11 43:12 61:8, 11 Baehr 4:8 14:1 17:13, 14 54:7, 10, 13, 20 Baehr's 55:3 BANNER 3:15 5:24
---	---	--	--

based 22:6 27:3, 7 32:3 33:25 34:18 40:10 basic 51:19 basically 19:1 35:16 39:24 46:17 52:13 54:23 basis 30:9 40:22 58:7 59:10 Beginning 1:17 21:18 begins 41:11 behalf 5:5 believe 10:23 15:12 18:10 19:19 21:2 26:9 34:2, 3 37:4 42:6 46:24 47:18 48:2 51:13, 14 53:16 64:17 belongs 21:24 22:4, 14 27:18 beneficial 26:19 benefits 54:21 best 7:18 44:24 45:8 66:13 better 44:4 49:7 56:11 bit 24:1 56:11 blacklist 28:10, 14 39:12 41:22, 24 42:10, 11 58:21 59:1, 6, 7, 20, 21 60:3, 7, 19 blacklisted 28:7, 16, 17, 20 29:24 30:17, 21 31:1, 5, 9, 11, 12, 20 35:19 41:4 42:5 59:14 blacklists 58:8 60:17 blanket 65:4 block 23:12 42:8 blocked 42:17	blocking 60:19 BOARD 1:2 bones 34:22 bottom 41:10 box 25:20 47:25 49:5, 7 50:4, 9 51:11, 12 52:10 53:17 boxes 49:4 51:6 53:12 break 36:2 60:25 bring 11:20 broad 28:11 29:20 33:2 49:1 built 18:25 28:21 45:4 bunch 44:10 Buru 4:8 13:21, 22 14:24 16:13, 14 17:3, 25 18:4, 7 21:1, 5, 10, 15 22:4, 18, 19 24:23 26:18 27:11 28:6, 10, 18, 21, 23 29:10, 16 30:3 31:25 32:12, 18 33:11, 13, 24 34:1, 3, 7, 10, 15 35:9, 15, 24 37:3, 13 38:22, 24 42:2, 4, 6, 21 43:1, 3 47:21 48:1 50:4 57:20, 24 59:13, 14, 17 60:12, 16 Buruganahalli 12:11 Buru's 22:12 30:4 36:18 < C > CA 2:14 3:11 call 8:6 48:24, 25 called 38:4 39:7 calling 13:20, 22 40:20	can 6:5 7:25 11:19, 20 12:22 16:12 19:21, 25 20:4, 25 21:5 22:5, 19 23:5, 18 25:3, 4, 5, 16 26:10, 24 27:4, 12 33:10, 13, 19, 20 36:14, 22 38:8, 20, 25 39:1, 4, 12, 13 40:6, 8, 13 44:1, 11 45:21 46:11 47:21 52:7 55:22 57:11, 19 64:20, 21 cannot 38:23 can't 15:8 19:22 37:9 CAPTION 4:2 captured 19:4 capturing 19:1 carried 35:8 49:24 51:17 carries 50:14 carry 51:20 CASE 1:3 4:2, 15 5:22 8:10, 23 9:21 10:17 11:8 15:4 17:24 32:19 37:7 44:16 47:9 50:15 52:20 55:6, 20 56:9 64:25 65:3 cases 45:18 60:22 cause 38:14 66:15 central 5:10 CENTRIPETAL 1:6 4:8 5:22 63:9, 16 certain 10:24 16:7 17:11, 12 20:21 22:16 24:3 39:8, 9 51:20 62:3, 13 63:12	certainly 24:20 34:24 39:20, 23 45:7 50:24 59:11 CERTIFICATE 4:4 certify 66:7 challenge 46:18 challenged 8:22 change 65:3 changed 8:17 characterize 30:13 chat 14:16, 18 21:7, 13 cheaper 44:8 check 16:6 25:19 27:21 28:1, 15, 18 29:23 30:15 31:2 34:4 35:17 41:22 52:6, 7 63:12 checked 30:25 33:4 Checking 31:18 Cheryl 1:15 66:4, 21 Chicago 3:17 choose 42:8 chosen 27:7 CHOW 2:12 6:2 8:6 circulated 8:16 Cisco 4:8 62:18 63:9, 16, 22 citation 37:17 cite 38:20 cited 9:21 ckronenthal@bann erwitcoff.com 3:17 claim 9:18 57:16, 17 claims 8:20 9:1, 5, 10, 11, 14, 22 10:4, 8, 12, 19 12:3, 5 46:18 59:18 64:7
--	---	---	---

clarification 20:15 35:13 46:6 53:11 clarify 46:21 53:7, 11 clean 12:20 13:4 14:8, 9, 11 15:18 clear 7:15 11:24 23:2 24:13, 22 25:8, 14 29:7 32:20 37:25 64:15 clearly 24:10 37:23 58:23 client 46:3, 7 collection 35:3 collectively 32:13 40:20 Column 21:15 22:25 23:7, 9, 21 25:5, 25 26:10 29:13 33:10, 21 37:18 38:21 39:25 40:6 58:4 59:4, 6 come 42:14 49:19, 21 comes 57:5 Commission 66:24 common 20:22 45:19 communicated 53:1 communicating 45:7 48:15 communication 20:3 40:13 47:2 communications 17:22 complete 7:19 completely 10:24 14:11 23:2, 4 24:13, 22 25:8 32:21 38:6 completion 14:25	component 33:5 38:3 39:7 47:13 51:1, 3 53:1, 21 54:4 components 46:12 computer 45:14 59:25 Computer-Aided 66:10 concept 34:25 49:2 concern 57:22 concerned 58:9 concerning 60:15 conclude 47:2, 19 48:3 concludes 52:17 65:19 conducted 5:11 20:19 confirm 15:13 16:10 conjunction 17:19 conjunctive 59:9 connected 27:13 connection 47:12 connections 44:7, 10, 11, 18, 20, 25 45:10 consider 62:2 considerations 61:17, 24 62:8, 22 64:4, 19 65:2, 6 considered 9:20 63:1 consistent 55:11 consists 29:21 construction 56:12, 13, 14, 22 57:4 58:18 constructions 55:10, 17 construe 46:20, 21 55:12 construed 55:6,	20 56:8 construing 51:25 consult 31:13 32:1 35:5 consulted 35:11 contain 37:15 66:11 CONT'D 3:1 contend 47:25 content 19:19 39:22 context 34:4, 5 48:13 50:3 58:8, 25 continually 65:8 continue 44:23, 24 conventional 49:23 convincing 64:16 copies 12:18, 20 13:9 14:14, 19 copy 13:4 15:18 correct 9:2, 3, 19 12:11, 12 13:7, 12 14:4 20:16 21:1 22:7 23:13 25:22 30:12 32:10 35:7 36:18 54:8 63:19 66:12 correlate 32:16 41:7 correlated 27:14 28:7 35:21 correlates 30:16 correlation 30:1 35:17 41:3 corresponds 27:22 28:2 41:15 could 16:4 23:3 24:18, 20 26:2, 3 42:8 49:15 53:3, 14 54:24 56:11 58:12, 15 59:8, 11 couldn't 52:5 counsel 8:4, 12,	14, 25 18:7 66:16 COUNTY 66:3 course 9:8 22:17 42:9 59:8 Court 3:22 5:6 6:4 20:14 35:12 46:5 65:15 courtesy 7:21 CPU 54:4 CRAIG 3:15 5:24 created 38:15 56:14 criteria 57:18 critical 26:24 CRR 1:15 CT 1:17 cuff 42:25 current 64:22 < D > data 18:24 37:1, 8, 9 38:19 39:1 49:4 57:18 date 5:9 15:3, 9, 11, 16 16:3, 10 DC 2:8 decide 42:12 decided 53:19 decision 40:2 47:9 52:14 62:4 decisions 40:3 47:14 Declaration 4:8 8:2, 10, 19 12:24 13:6 15:1, 10, 11, 16, 20 16:16 18:14 21:6 36:15 43:19 51:13 52:23 55:23 61:14 63:11 decoder 23:22 24:2, 15 51:7 decodes 23:23 24:15 decoding 24:2 51:5
--	--	--	--

decrypt 38:23, 25 40:4 60:15 decrypted 37:10 40:5, 15 43:8 52:18 55:2 decrypting 39:21 47:13 52:8 decryption 37:15 38:2, 4, 5, 9, 15 39:7, 13, 20 43:9 47:1, 4, 25 50:10, 24 51:2 52:15, 19, 25 53:17, 23, 25 54:11, 15, 22 deep 9:15 deeper 60:20, 21 defendant 10:14, 20 depend 48:13 depending 46:13 depends 48:9 50:1 52:1 deponent 5:7 deposed 6:17, 20, 23 7:2, 4 DEPOSITION 1:6, 14 5:5, 7, 11 65:20 describe 33:7 44:1 57:20 59:14 described 29:13 32:18 38:12 39:5, 6, 24 41:2 49:9 51:8 describes 21:23 33:24 54:13 57:17 58:6 59:6 describing 21:25 43:6 58:22, 25 description 23:11 destination 20:9 23:1, 15 24:4 26:13, 20, 24 33:25 34:16, 18 39:11 43:6 59:7,	15 destinations 20:4 details 11:15, 19 62:20 detect 39:1 determination 31:8 35:22 62:1 64:11 determine 21:23 22:14 24:19 30:15 39:13 40:8 41:2 44:3, 22 45:10 48:18 determined 22:3 24:8 26:3, 7 31:5 32:4, 16 40:11 60:8 determines 22:21 25:25 27:18 42:23 determining 22:5 develop 19:11, 12 developing 19:12 device 22:13, 21 25:10 30:4 51:24 53:10, 13 54:12 devices 49:24 diagram 23:12 did 8:1, 5, 9, 11, 20, 24 9:10, 14 10:2, 7 11:7, 9, 16, 21 12:4 14:23 15:15 16:14, 25 17:2, 10, 24 18:1 19:3, 11, 12 46:16 57:7, 9 didn't 9:24 11:11, 18 12:7 13:12 46:20, 21 differences 12:4, 8 different 28:12 29:22 39:5 42:6, 7 43:17 45:17 46:12, 13 48:20 differentiates 50:7	differently 41:8 difficult 7:16 DIGITALLY-RECORDED 1:5, 13 DIRECT 4:4 6:9 directed 46:9 directly 17:6 32:18 52:16 discern 12:4, 7 disclose 22:20 54:10 discloses 22:5 38:24 57:20 discovery 16:9 discuss 14:15 25:4 discussed 25:7, 20 28:23 29:8 discusses 21:1 24:2 discussion 21:19 22:25 36:17 55:14 57:4, 16 58:8 disjunctive 59:9 distinction 50:13 Dkt 4:15 Do 5:13 7:18 8:13 9:4, 7, 24 12:18 13:19 14:7 15:3, 6, 25 16:2, 7 18:2, 6, 19, 20 19:21 21:2, 19, 21, 22 23:21 24:7, 11 25:17, 18 26:14, 15 27:5 28:24 29:2 31:13, 16, 17 32:17 36:7, 21, 24 38:10, 17 40:2 41:12, 14 42:14, 21 43:15, 16, 24, 25 44:13 45:21 46:14 49:15 50:20 52:4, 13, 20 53:8 55:25 56:5,	18 57:20, 24 58:15 60:20 61:17 62:10, 24 64:8, 9 66:6 document 12:14 13:14 14:1, 16 15:24 documentation 16:11 documents 11:15 12:19, 21, 22 14:5, 8, 15, 17 29:8 Does 7:22 22:14 23:14, 16 24:23 25:11 26:18 27:2 28:18 30:20 32:19 34:22 36:19 37:2, 14 41:14 42:4, 21 45:13 54:10 56:6 59:14, 17 60:6, 24 61:22 doesn't 14:19 24:10 52:13, 15 54:15 doing 7:16 26:3 49:16 50:2 51:1 53:4 Dolphin 3:10 domain 23:15 24:4, 11 25:11 26:4, 6, 13, 20, 24 27:14, 22 28:3, 7, 17, 20 30:16 31:21 32:16 33:25 34:16, 19 35:18 39:11 41:4, 8, 22, 23 43:7 59:7, 20 60:16 domains 23:1 59:15 done 23:2, 3 24:22 33:15 42:1 44:22 49:13, 14 50:20, 25 51:23 65:14
--	---	--	---

don't 11:14, 18 12:16 13:2, 8 14:5, 9 15:5 16:3, 15, 21, 23 17:21 19:8 24:12, 13, 16 26:9 28:25 31:10, 12 33:17, 21 34:6, 12 37:12 41:6, 9 42:24 43:15 51:7 56:10, 15, 17 57:3, 6 58:5 60:4, 5 62:20 63:4, 7, 13 64:23 65:10 DOUGLAS 66:3 down 24:1 33:14 41:10 58:5 Dr 5:8 6:11, 16 7:25 8:9 36:14 draft 34:12 drafts 8:15 drill 7:9 Drive 3:10, 16 duly 6:7 during 16:15 < E > E.D 4:15 earlier 23:17 25:8, 21 28:8 35:4 39:3 41:2 49:6 early 26:14, 17, 20 easier 29:1 easily 54:24 East 2:14 eavesdropping 55:1 edge 43:24 44:2 eight 7:8 either 17:5, 15 18:3 22:21 element 53:9 elements 53:14 eliminate 45:23	embodiment 22:18 25:2 38:11, 25 41:6 embodiments 25:2 37:24 39:6 42:7, 12 enables 33:3 encrypted 19:4, 9, 13, 17, 21 28:5, 15, 18 31:11 35:10, 14, 22 37:1, 8, 9 38:19, 23 39:9, 12 40:12 41:2, 7 42:13, 18 43:8 52:6, 7 60:13 encryption 52:13 engaged 15:4 16:1 engine 21:19 23:23 24:2, 15 25:25 37:15 38:4, 16 39:7, 13, 20 43:9 47:1, 4 52:19, 25 53:17, 23 54:11, 16, 22 entire 48:5 entity 53:1 essentially 27:17 30:6 42:7 establish 24:11 29:25 44:6, 10 45:11 establishing 25:11 event 66:17 ever 6:16, 23 7:4 10:17 24:21 every 60:19 everybody 50:18 everybody's 29:1 everyone 21:8 36:8 everything 32:21 evidence 26:15 62:6, 7, 14 64:6 65:2 exact 16:3	exactly 22:9 25:15 EXAMINATION 4:4 6:9 examined 6:8 examining 39:21 63:5 example 22:24 32:15 38:13 39:10, 25 45:22 49:6 52:20 54:15 57:11, 16, 19, 23 58:13 examples 46:2 47:18 except 59:18 executed 15:24 executing 32:12 execution 34:23 Exhibit 4:8 12:14, 16 13:1, 3, 7, 17, 23 14:3 17:15 21:11 54:8 63:1, 15 EXHIBITS 4:8 21:7 62:25 exist 53:14 exists 64:12 expensive 53:25 experience 18:21 expert 6:24 7:2 10:2 Expires 66:24 explain 19:25 explanation 23:19 expose 26:18 expressly 39:6 59:17 extend 7:21 extensive 10:1 extent 62:13, 17 64:3 extract 26:19 extracted 26:6 extracting 23:1 26:12	extraction 23:15, 20 24:4, 12 25:12 34:17 extremely 64:16, 17 < F > face 18:4 49:11 Facebook 59:25 60:2 fact 60:6 factors 62:3 faculty 18:25 fairly 20:23 49:23 familiar 12:10 46:2 54:7 far 25:10 33:7 34:11 41:5 FAX 3:23 feel 29:5, 7 feeling 64:22 fetch 46:4, 8 fewer 10:18 Figure 23:12, 17, 18, 22 25:16, 17 36:18, 21 37:12 38:2, 8 47:21 52:7, 10 53:8 filed 11:8 15:17 filtering 29:21 33:4 34:4, 24 38:13 39:17 40:2 41:16, 17, 18 57:21 58:7, 23 59:10 filters 41:12 final 14:1 find 10:3 57:16, 24 fine 13:22 33:17 36:3 fingertips 29:3 finish 7:22 firewall 36:22 37:10, 13, 14, 19 38:2, 3, 8, 12, 25
---	---	---	--

39:1, 4, 8 40:1 41:11, 14 48:5, 9, 12, 19, 21, 24 49:1 51:17, 19 52:5, 7, 12 53:13, 23 54:1, 11 firewalls 37:10 38:18, 22 49:25 first 6:7 15:3 22:13, 16 24:10, 21, 24 25:3 52:9 flavors 42:8 Floor 2:13 flow 19:18, 20 20:1, 2, 11, 18 21:1, 23 22:1, 4, 14, 22, 23 24:7, 9, 11, 17, 20, 23 25:9, 11, 13, 14, 21 26:1, 2, 7, 14, 16 27:4, 6, 7, 12, 17, 19 30:3, 7, 11, 23 31:6 32:24 40:11, 13, 16, 21, 24 47:2 49:5, 6, 9, 11 50:9, 11 flows 21:2 23:23 24:16 30:20 focused 11:15 folks 48:25 follow 44:5 following 5:1 follows 6:8 55:3 force 39:18 foregoing 66:7, 10 form 10:6 11:4 12:6 18:8 19:6, 15 20:13, 20 22:8 26:21 34:9 35:23 44:20 52:11 63:20 forth 59:1 found 44:24 frame 15:7 17:22 FRANKEL 3:5,	10 free 29:5, 7 front 12:19, 23 13:10, 14 14:6, 19 29:9 full 7:19 9:13 17:16 66:11 FULLER 3:6 5:23 function 49:12, 24 50:14, 15, 22, 23 51:2 functionality 50:10, 12 51:5, 19 52:9, 16 functions 27:15 48:21, 22 49:14 51:21, 23 52:2 further 24:1 34:17 39:22 40:15 42:14 47:14 52:20 65:11 future 45:19 64:14 < G > General 1:15 15:6 65:7 66:5, 22 generally 20:2 getting 55:1 give 7:19 11:11 42:24 45:22 54:15 given 8:17 10:1 16:16, 24 17:6, 7, 17 18:11 26:13 30:11 50:4 54:22 go 12:18 13:1 23:18 25:5 29:12 33:14 43:12 52:20 goes 26:22	going 7:9, 11, 18 30:24 36:1 37:21 41:19 60:20, 23 Good 5:3 6:11, 13 7:23, 24 14:13, 21, 22 36:2 58:21, 22 60:25 61:1 grant 18:24 GRAY 2:7, 12 6:1, 3 8:4, 5 guess 6:22 20:25 23:7, 8 29:14 43:14 58:5 60:6 gun 54:2 GUY 3:21 5:4 < H > had 5:2 8:3 18:2, 23 19:9 23:17 handshake 36:23 41:20 42:16, 22 60:19 happen 41:23 happened 47:16 happening 22:20 24:6 25:15 26:16 51:24 happens 25:3 33:7 50:8 happy 16:7 hard 14:14 has 11:2 18:18 20:8 27:23 28:8 31:25 32:18 38:12 42:6 46:22 48:25 51:22 52:1 54:1, 18 55:6, 19, 21 56:1, 8, 15, 19, 24 60:8 have 6:16, 18, 19, 23, 25 7:1, 4, 6 8:20 9:4, 10, 24 10:17, 19, 23 12:1, 18, 20, 23, 24 13:4, 14, 19, 20 14:1, 5,	9, 13, 16, 17, 19 15:6 16:4, 6, 10 17:11, 25 18:2, 5, 6, 9 19:7, 17 20:11 21:5 29:2, 9 31:2 33:18 34:6, 21 36:7 37:7 39:14 41:10 45:13 46:10 47:16, 17 48:11 52:15 61:6 63:2, 3, 23, 24 65:5, 10 haven't 50:4 he 34:16 header 20:12 helps 37:20 hereunto 66:18 highlighting 14:10 history 10:1 honestly 12:16 15:8 56:17 host 23:19 29:17 45:6 hour 36:2 60:24 HTTPS 60:14 < I > ID 20:2 idea 15:6 47:16 57:24 identification 25:21 IDENTIFIED 4:8 26:17 identifiers 29:17, 19 identifying 49:10 identity 56:3 57:14 58:2, 9, 19, 24 IDs 19:18, 20 20:1 if 11:20, 25 13:2 14:15 16:7, 15 17:21, 23 19:8, 22 20:7, 11 21:15
---	--	--	--

24:6, 19 25:1 28:24 29:25 31:4, 11 37:20 39:10 40:11 41:2, 3, 20, 21, 22, 23 42:9, 11, 16, 21 43:6, 15 44:4, 9, 18 45:9 48:9, 21 49:12, 13, 15 52:5 53:18 55:21 60:11 IL 3:17 implementation 52:4 implemented 32:1 39:4 60:4 important 27:14 improve 54:5 included 18:18 63:17 includes 34:17 37:17 including 9:14 incoming 35:6 independent 12:5 INDEX 4:3 indication 20:3 57:22 indicator 56:1 57:10 58:1, 13, 16 59:13 indicators 55:19 56:2 57:13 58:18 indicia 63:18 individual 49:3, 4 53:13 information 20:12 26:12, 19, 23 35:21 48:17 63:17, 25 64:12, 13, 24 informed 62:21 infrastructure 18:25 Infringement 10:16	initially 36:22 40:10 initiated 55:7 initiation 55:20 56:9 input 8:20 insert 8:18 inside 41:21 inspect 36:23 38:19 inter 7:5 interactions 18:3 interested 66:17 interesting 48:8 interior 44:18 intermediary 44:17 45:20, 21, 23 46:17, 23 47:17 50:1 intermediate 44:6 Internet 16:18 interpretation 57:12 interpreted 56:2, 15, 19, 24, 25 59:8 introduce 5:18 intrusion 18:19, 22 43:23 invalid 64:22 invention 35:1 37:14 62:1 inventors 18:3 involve 19:3 involving 39:17 62:18 IP 20:5, 8, 9 21:19 22:6 25:19, 25 29:18 35:24 44:5, 12 45:8 IP-3 53:2 IPR2022-00182 1:3 IPRs 10:7 isolated 54:18 issue 34:7 62:21 item 43:23	its 31:9 48:12 49:11 54:4 < J > JEFFREY 3:4 5:20 JENNA 3:6 5:23 jfuller@kramerlevi n.com 3:13 job 51:8 joined 5:23 6:2 joint 18:23 JON 1:6, 14 2:3 5:8 6:6 66:7 Jones 3:22 jprice@kramerlevi n.com 3:6 judgment 48:11 jump 20:25 June 4:16 16:5 < K > keep 31:15 59:5 key 50:22 KEYNA 2:12 6:2 8:6 keyna.chow@ropes gray.com 2:16 keys 54:23 kin 66:14 kind 14:10 44:24 45:23 46:11 48:14, 17 49:1 50:22 51:19 knew 45:6 know 7:9, 15 8:16 15:9 18:2 25:9 29:23 31:2, 10, 12 33:15 34:11, 21 45:3, 19 46:11 47:7 48:9, 13, 21 49:11, 16 50:17, 19 51:18 52:3, 17, 22, 23, 24 54:16, 20, 22, 23 56:13, 15, 17 57:3,	6, 21 58:5, 6 59:8 60:4, 5 62:19, 20, 21 63:21, 24 64:18, 23 Knowing 27:13 knowledge 17:25 known 23:22, 24 24:14 KRAMER 3:5, 10 5:23 KRONENTHAL 3:15 5:24 < L > language 8:18 42:25 57:3 large 39:16 larger 49:10, 23 latencies 45:4 lead 47:5 legal 8:18 level 44:11, 12 53:2 levels 29:22 LEVIN 3:5, 10 5:23 life 29:1 line 14:18 21:18 22:3 23:9, 10, 20 25:6 26:11 33:14, 19 38:21 40:6 Lines 23:7 29:14 33:22 39:25 43:5 list 42:23 43:7, 16, 23 62:25 listed 18:3 litigation 10:9, 11, 15 62:9, 12, 18, 19 litigations 10:16 little 24:1 56:11 LLP 3:5, 10 locate 16:14 logs 19:8 long 15:25 look 9:13 11:9, 20 19:18 25:9
---	--	--	---

29:24 35:16 41:20, 21 43:1 46:22 47:17 48:11 52:1 54:17 60:15 looked 19:23 looking 22:17 26:4 29:10 48:18 Looks 61:5 look-up 32:3 lot 15:9 29:1 54:21 < M > machine 29:4 Madam 6:4 main 61:6 major 12:4, 8 making 47:9 management 50:21 MARKED 4:8 12:14 13:9 markings 14:10 matches 59:20 matching 32:24 materials 16:21 62:25 matter 6:24 7:2 16:1, 21 57:5 62:15, 23 63:22 matters 10:2 56:17 MCKEOWN 2:6 5:16, 25 8:8 10:6, 21 11:4 12:6 18:8 19:6, 15 20:13, 20 22:8 26:21 34:9 35:23 36:10 52:11 60:10 63:20 65:14, 17 mean 8:13 14:9 19:11, 25 30:6 31:16 34:22 37:2, 5 40:7 45:21, 24	51:16 52:2 53:2, 10 56:2, 10, 15 58:15, 17 60:8 63:2 meaning 30:17 43:16 45:14 46:16 55:16 57:9, 13 means 24:16 34:1, 4 35:1, 19 37:3, 22 56:21, 25 meant 53:11 meat 34:22 meet 8:5 meetings 8:4 memory 15:16 mentioned 35:4 mentioning 62:11, 12 merely 49:9, 16 midst 63:10 mind 13:2 28:24, 25 mine 8:19 mining 18:24 MOBILE 1:5, 13 monitored 26:1 monitoring 21:25 22:12 months 16:2 morning 5:3 6:11, 13 8:1 motivation 54:17 55:3 move 13:13 16:12 moving 54:10 multiple 44:6, 25 < N > NAFTALIS 3:5, 10 name 5:4, 20 23:19 26:4, 6 28:7 30:16 60:16 names 29:17 naturally 44:5	Nebraska 1:16 3:23 66:2, 6 necessarily 37:21 49:12 60:7, 18 necessary 65:17 need 7:11 40:4 48:14 62:3 needs 40:4 42:13 52:14, 18 network 18:18, 22, 24 22:12, 21 43:22 45:5 46:12 48:14 49:24 51:11 52:3 54:5 56:4 57:15 58:2, 12, 20 59:16, 22 60:1, 9, 18 65:7 networking 45:15 NETWORKS 1:3, 6 5:22 6:1 11:3, 13 43:24 44:2 network-threat 55:19 56:1 57:10 58:13, 16 59:12 never 9:20 New 3:6 22:22 23:8 25:9 26:13 35:6 40:9 59:24 NO 1:3 4:15 8:21 9:24 11:18 12:8 14:13 18:5, 9 30:24 47:16 61:20 65:1, 17 nodes 45:5 nonobvious 63:18 normal 52:3 Notary 1:16 66:5, 22 notes 14:9 44:6 notice 13:12 November 15:12, 13, 25 66:24 NSF 18:23 number 10:18 16:17 17:6, 17 19:20 22:7 26:1	28:12 45:17 54:13 numbers 12:17 13:9 20:5 33:19 numerous 51:14 NW 2:7 NY 3:6 < O > Objection 10:6, 21 11:4 12:6 14:13 18:8 19:6, 15 20:13, 20 22:8 26:21 34:9 35:23 52:11 60:10 63:20 objective 62:3 63:18 obvious 9:23 46:19 52:24 53:3, 20, 22 62:1 64:20 obviously 19:21 25:12 56:13 obviousness 64:6, 15, 24 occasion 9:10 occurs 23:15 24:7 26:5 odd 10:3 off 36:4 42:25 61:2 offered 55:17 OFFICE 1:1 59:23 officially 56:16 Oh 13:11 61:18, 20 Okay 7:4, 14 11:10 13:13, 25 14:13 17:8 18:16 21:17 22:2 27:5 29:6, 12 30:2 31:4 33:23 34:6 38:24 55:24 56:6 57:7, 13 61:15, 16
---	---	--	--

62:5, 24 63:14 64:2 65:1 old 22:23 Omaha 3:23 once 31:22 44:23 ongoing 65:7 Online 1:15 open 29:4 54:24 operation 53:25 opine 55:9 opinion 9:1, 6, 17, 24 10:18 26:8 64:5, 15 opinions 8:18 9:9 10:4 12:2 opposite 23:4 optimal 44:23 order 23:1 24:21 26:5 34:25 44:22 51:9 65:18 orders 65:15 ordinary 34:2, 14, 20 35:2 37:4 45:24 46:24 47:5, 19 48:3, 4 49:17 55:12, 16 58:11 59:11, 19 62:2 origin 46:4, 8 original 38:17 outperform 44:11 outset 15:1 outside 37:22 53:14, 23 54:11 outweigh 64:5 OWNER 1:8 3:4 5:21 10:13 62:8 64:3, 13 owner's 11:7 < P > p.m 61:4 packet 18:18, 21 20:7, 10, 12 21:24 22:3, 4, 13, 14, 22 24:8, 21, 24 27:8, 13, 18, 22 28:2, 5,	6 29:21 30:8, 15 31:1, 4, 7, 9, 11, 19, 24 32:2, 15, 24 33:3 34:4, 24 35:6, 10, 15, 16, 18, 22 37:6 38:13 39:17, 19, 21 40:1, 4, 24, 25 41:18, 24 42:16, 22 43:22 44:21 45:12 47:14, 15 50:8, 11 55:2 packets 19:1, 4, 8, 13, 17, 21 24:19 28:15, 19 30:7, 11, 23 32:13 38:15 40:17, 18, 20 41:4, 7, 12, 15, 19 42:5, 14, 18 43:8 49:10, 22 50:17 51:8 52:6, 8 54:1 60:13 Page 4:2, 3, 4 13:10 14:21 15:19, 21, 22 18:15 21:8 33:12 36:20 37:17 38:7 41:10 46:4, 8, 10 61:22 pages 61:13 66:11 PALO 1:3 2:14 6:1 11:2, 12 Paragraph 18:15, 17 23:8 25:24 26:23 33:21 36:15, 17 43:5, 14, 18 55:22 59:1, 2, 3, 5 61:19, 21 62:5 64:2 parenthetical 36:25 part 9:21 20:11 22:22 24:8 25:13 27:8, 21, 23 28:1 31:5 32:6 35:7	39:23 48:10 49:10, 22 50:17 53:12 57:3 partes 7:5 particular 18:15 21:24 24:9 27:7, 14, 22 28:2, 16, 19 30:5, 25 41:1 47:9 48:19 50:9, 14 63:5 particularly 53:17 parties 5:12, 13, 18 66:15 pass 45:9 passage 21:22 23:16 26:10, 12 34:8 passages 37:18 passed 43:10 PATENT 1:1, 2, 3, 8 3:4 4:8 5:21 6:24 7:2 8:3, 21, 22 9:12, 18, 23 10:2, 5, 13, 15 11:2, 7, 12 12:4, 25 13:5, 16, 21, 23 14:2, 3, 24 16:13, 14, 17 17:1, 4, 6, 7, 16, 17, 20, 25 18:4, 7, 11, 12 21:1, 6, 10, 16 22:4 29:16 34:11, 12 37:23 46:19, 25 55:6 57:17 62:8 64:3, 6, 13 patentability 9:1, 9, 17 12:3 26:8 patents 9:13 34:12 path 44:7, 23, 24 45:11 47:8 patterns 60:15 PDF 28:24 29:4 Pennsylvania 2:7 people 46:3 51:10 65:8	perform 16:25 38:4 46:12 51:22 performance 54:3, 5 performed 51:10 52:10 performing 27:15 48:22 performs 38:2 permissible 40:11 per-packet 40:22 person 34:2, 14, 20, 21 35:2 37:4 45:24 46:24 47:5, 18 48:2, 4 49:17 55:11 58:10 59:11, 19 62:2 persuasive 64:16 petition 63:4 PETITIONER 1:4 2:6 phenomenon 44:9 pick 43:3 place 22:19 25:5 58:4 places 22:24 42:2 51:14, 16 plain 55:15 plane 49:4 playing 46:23 47:1 please 5:18 6:5 29:5, 7 36:14 43:2 point 14:23 22:19 23:5 24:20 25:3, 13 32:25 38:8 50:20 57:1 pointed 16:24 pointer 17:6, 17 18:11 points 44:4 45:1 47:10, 16 48:7 50:16 policies 22:5 27:3, 5, 9, 11, 18
---	---	---	--

29:17 30:21, 22 32:20 33:2 51:12, 14 policy 27:21 28:1, 3, 6, 10, 11, 14 29:20, 21 30:5 31:6, 23 32:7, 9, 11, 14, 23 33:7, 8, 25 34:3, 8, 18, 22 35:2 39:1, 14, 16, 23 40:10, 14, 23 51:6, 16 52:6, 8, 10, 16 58:7 port 20:5, 8, 9 21:19 22:6 25:20, 25 26:1 35:25 portion 29:16 38:20 position 52:23 53:16 65:1 possible 7:15 26:14, 17, 20 30:25 41:8 45:8 48:23 49:15 64:18 65:2 Possibly 8:16 48:12 potential 19:2, 5, 14 39:19, 22 59:22 60:12, 17 potentially 42:15 47:10 54:25 preferable 45:11 preliminary 11:8, 10 preparation 16:16 63:10 prepare 8:1 preparing 12:2 63:11 presence 64:19 PRESENT 3:20 presented 62:8 Presumably 15:1 43:9	presume 17:3 59:25 presumed 55:15 previous 62:9, 11 PREVIOUSLY 4:8 43:21 PRICE 3:4 5:15, 20, 21 6:10 10:10, 25 11:6 12:9 18:13 19:10, 24 20:17, 24 21:5, 11, 14 22:11 27:1 34:13 35:20 36:1, 9, 13 46:15 60:23 61:7, 10 64:1 65:10, 18 Price.....Page 4:4 Principally 8:6 11:16 printed 14:11 prior 8:3 14:25 16:5 17:11, 24 39:19 40:12 43:22 55:10, 20 56:8 62:18, 19 Probably 7:8 50:5 63:3 problem 7:12 65:8 proceed 61:6 proceeding 7:5 12:15 64:4 proceedings 5:1 proceeds 25:19 process 54:1 processing 19:2, 4, 13 26:25 49:14 Professional 66:5, 22 project 45:3 protocol 20:6 23:22 24:2, 14, 19 40:9 protocols 23:24 24:3 34:17	provide 9:1, 6, 17 10:4 24:3 64:14 provided 10:8, 18 16:13, 18 17:4, 5, 15, 18, 19, 21 56:12 63:6, 9, 23, 24 provides 36:17 providing 9:9 proxies 44:20 45:17 54:18 proxy 43:23 44:1, 12, 14, 16 45:13, 22 46:3, 9, 11, 13, 17, 21, 22 47:3, 6, 19 48:1, 6, 19, 21, 23, 24 49:1, 7, 12, 18 50:3, 10, 12, 13, 22 51:3, 18, 20, 22 52:19 53:18 54:14, 21 55:5, 11 Public 1:16 63:17, 25 64:12, 23 66:5, 22 publicly 62:7, 14 put 14:17 34:21 53:24 putting 60:2 < Q > qualify 48:19 50:3 51:2 question 17:9, 13 27:16 38:12, 17 48:8 60:6, 17 questions 7:10, 20, 22 65:11 quick 43:1 quickly 33:11 54:2 quietly 33:16, 17 quite 64:25 quote 37:16 < R >	RADSCH 2:8 6:2 8:7 read 11:22 12:1 23:17 26:2 33:18, 20, 23 35:2 59:12 reading 24:12 30:18 33:14 37:16 43:11 ready 61:6 realized 53:3 really 50:4, 22 53:5 63:4 re-answer 17:9 reason 54:3, 6 reasonably 47:2 59:12 reasons 54:13 recall 11:14 15:3, 5, 8, 25 16:15, 21, 23 19:8, 22 37:13 41:6, 9 57:3 63:4, 7, 13 recalling 25:1 receive 20:7 received 24:24 28:5 31:4 35:10, 15 42:18 receiver 47:8 receives 22:13 42:22 Recess 36:6 61:4 recognize 53:8 recognized 24:17 30:4 recognizes 25:12 recognizing 25:10 recollection 18:10 56:7 record 5:4, 19 7:14 11:24 12:13 33:16, 18 36:5, 12 61:3, 9 64:13 65:16 recorded 41:25 recording 5:5
--	--	---	--

records 16:6 reduced 66:9 Redwood 3:11 refer 8:21 15:15 17:16 38:20 41:16 49:18 61:24 reference 12:11 17:14 47:22 48:1 54:8, 17 63:5 referred 15:19 28:10 32:9 referring 14:14 23:6 24:18 28:3, 9 29:15 37:13 38:7 40:8 62:15 refers 26:12 53:9 58:11 refresh 15:15 56:6 Registered 66:4, 22 reiterating 27:10 relate 60:14 relevant 17:1 26:7, 24 34:5 remember 11:19 12:16 13:8 16:3 17:21 remembered 41:25 42:3 remotely 1:14 2:2, 5 3:3, 21 5:13, 14 rendered 9:22 repeat 33:19 REPORTER 4:4 6:5 20:14 35:12 46:5 65:15 66:5, 22 Reporters 3:22 5:6 represent 5:21 32:14 52:25 56:3 57:14 58:19	represented 20:4 31:19 40:17 representing 6:1 represents 58:1 reproduction 36:21 request 46:9 Requests 20:14 35:12 46:5 65:15 require 40:14 requires 50:19 resource 56:3 57:14, 22 58:2, 19, 24 resources 58:9, 10 respect 31:18 62:22 response 11:8, 10 restate 39:16 return 26:10 43:18 Returning 38:17 review 7:5 9:11, 15 11:7 reviewed 8:2 right 13:11 17:12 21:4 22:15 23:12 24:21 27:10 29:10 30:2 32:18, 23, 25 33:25 34:6, 8, 19, 20, 23 35:6 36:20 37:11 39:2 40:24 42:19 53:10 56:14, 21 57:1, 8 60:19 64:23 risk 54:25 role 44:14 46:22, 23 roles 46:13 Rooney 1:15 66:4, 21 ROPES 2:7, 12 6:1, 3 8:4, 5 Roughly 6:19	15:25 route 44:4, 21 routed 38:15 43:9 router 48:10 routes 52:18 routine 49:23 routinely 50:25 routing 43:24 44:1, 5, 7, 12 45:12 53:2 RPR 1:15 66:21 rule 29:23, 24 30:14 31:13, 15, 16 33:4 35:5, 7, 8, 15 39:2 41:1, 19 42:8 46:25 52:17 rules 27:24 29:22 30:7, 8, 11 32:1, 7, 12, 21 33:8, 9 34:5, 24 35:3, 5 38:14 39:17, 18 40:2, 3, 18, 19, 20 41:18 58:23 running 40:1 runs 35:15 < S > safe 17:3 saying 27:11 31:15 34:3 37:23 43:15 49:16 52:1 56:20 59:5 says 22:10 23:21, 25 24:5, 14 25:24, 25 27:11 34:16 36:25 43:3 52:17 scenario 44:15 scope 10:21 37:23 60:10, 12 SCOTT 2:6 5:25 8:7 scott.mckeown@ro pesgray.com 2:8 seal 66:19	search 16:25 17:10 28:24 29:5, 8 searched 17:11 second 20:10 37:4, 12 secondary 61:17, 24 62:7, 21 64:3, 19 65:2, 6 section 30:3 61:16 secure 34:17 40:9 security 18:24 26:25 27:15 39:22 53:9, 13 54:21, 25 65:7 see 11:16 18:19 21:20 23:21 24:21 25:17 26:14 29:25 36:21 38:10 41:12, 22 43:24 47:23 48:14 52:1 55:25 56:5 61:17 62:10, 24 64:8 seeing 25:1 63:7, 13 seen 27:23 28:8 64:11 sees 28:6 send 39:8 sender 47:8 sending 39:19 sense 50:2 sent 16:22, 23 39:12 sentence 41:11 separate 52:25 53:20 54:12, 14, 18 sequence 40:17 series 7:10 44:19 server 46:4, 8 session 20:3 24:25 37:7 38:14 39:10 40:9, 15, 16
--	---	---	---

42:9, 17, 19 49:11 50:18 54:23 sessions 60:14 set 10:12 27:3, 6, 12, 19 32:12, 20 33:8 42:13, 17 44:12, 17 47:11 sets 45:10 setup 37:6 40:12 48:15 Shores 3:11 shorthand 66:8 should 40:9 59:21 show 57:11 shown 23:22 signature 15:22 66:19 signatures 19:18 similarly 41:5 sit 46:11 sits 47:7 48:6 Sitting 10:22 11:14 19:22 59:23 situation 48:12 sixty-six 66:11 skill 34:2, 14, 20 35:2 37:5 45:24 46:24 47:5, 19 48:3, 4 49:17 55:12 58:11 59:11, 19 62:2 skim 11:21, 25 12:1 skip 11:18, 21, 25 skipped 11:17 sloppy 57:2 somebody 55:1 56:13 sorry 11:21, 23 13:6, 11 19:12 23:9 38:10 43:13 49:20 59:5, 6 61:18, 20 sort 9:15 26:3 42:7, 14 44:17	45:20 46:10 48:9, 16 51:16 54:17 58:4 sound 7:23 14:21 60:25 Sounds 7:24 14:22 36:3 61:1 source 20:5, 8 South 3:16 speak 40:16 special 51:21, 22 52:2, 9 specific 42:25 45:5, 6 54:15 specified 32:17, 21, 24 spelled 23:4 split 38:14 44:18 Ss 66:2 SSL 47:12, 24 60:14 SSL/TLS 37:7 Standing 65:18 start 33:13, 21 starting 22:2 23:7, 20 25:6 26:11 38:21 61:20 starts 25:17 State 1:16 18:17 42:3, 13 55:25 62:5 64:2 66:2, 6 stated 39:3 statement 63:22 65:5 STATES 1:1 stating 38:22 step 25:14, 17 49:6 stops 60:1 straight 58:18 Street 3:22 strength 64:20 strong 64:5, 17, 21, 25	subject 41:1 submitted 8:10 subsequent 26:4 37:6 38:13 43:7 subset 10:4, 8 sufficient 54:16 Suite 3:11, 16 summarize 30:2 summary 23:11 supposed 46:14 sure 7:17 11:25 12:24 30:13 33:11 38:6 44:3 53:5 57:25 swear 6:5 sworn 5:14 6:7 system 55:5, 11 < T > table 28:21, 23 29:13, 15, 25 30:5, 10, 14, 15, 17, 20, 24 31:2, 3, 6, 10, 13, 18, 20, 23 32:2, 4, 10, 17, 18, 22, 25 33:1, 3 35:5, 11, 16, 18 42:1 tables 45:4 take 11:9 32:2 41:19, 21 43:1, 2 49:5 53:22 58:10 60:13 taken 1:14 32:15 33:5 36:6 61:4 66:8 talk 37:18 talked 42:2 49:5 talking 7:17 25:23 26:11 33:12 34:15, 23 59:9 talks 21:2 22:25 34:7 54:20 61:16 tangible 34:25 TCP 50:19	teach 24:23 42:21 teaches 33:13 team 61:6 technical 34:21 technique 19:17 techniques 19:11, 13 24:3 tell 7:25 12:22 16:11 20:10 tells 30:10, 14 31:6, 23 52:14 temporal 17:22 ten 7:8 ten-minute 60:24 term 28:11 29:21 44:19 45:13, 16, 24 46:16 48:24 49:8 51:25 55:5, 10, 13, 16, 19 56:1, 8, 18, 19 termination 57:8 terms 25:10 54:2 testified 6:8 TESTIMONY 4:3 7:11 8:1 66:7, 12 text 54:24 Thank 6:13 13:13 21:12 29:6 61:12 65:11, 13 thereof 66:17 thing 22:13, 17 25:3 29:3 42:4 48:16 things 7:16 15:9 23:2 24:22 28:12 33:6 49:25 50:21 59:21 think 24:13 25:7 26:2 29:1 30:8 49:17, 25 50:3, 13, 18 51:7 52:23 53:10 55:2 56:10 57:2 59:10 60:11 62:15 64:17, 24 Thomas 3:22 5:6
---	--	--	---

thought 45:19 50:5 61:18 threat 56:4 57:15 58:3, 20, 22 59:18, 22 60:9 threats 19:2, 5, 14 39:23 58:25 59:16 60:18 three 12:5 tilt 64:21 time 5:10 13:2 15:6 16:22 17:22 36:2, 5, 12 43:2 61:3, 9 65:12, 20 times 6:19 7:1, 7 today 6:2, 12 7:10, 19 8:22 12:19, 23 13:23 14:6, 15 65:11 today's 5:7 65:20 ton 50:5 totality 32:6 touched 14:12 touching 63:17 to-wit 5:2 TRADEMARK 1:1 traffic 22:1 23:23 24:7, 15 36:23 38:23 39:8, 9, 12 41:20 50:20 Transcript 4:16 Transcription 66:10, 12 transcripts 63:8, 15 transport 44:10 treated 41:5, 8 Trial 4:16 63:9, 16 true 66:11 truthful 7:11 try 44:13 trying 47:11 53:6, 7	turn 18:14 21:15 25:16 33:10 36:14 37:3 40:6 47:21 55:22 61:13 Twin 3:10 two 8:3, 16 44:4 48:6 type 47:20 types 46:1 48:20 49:13 typewriting 66:9 typical 20:18, 22, 23 36:22 37:10, 13, 19, 22 38:10, 18 50:15 52:5 typically 38:23 48:23 51:23 52:4 < U > U.S 1:3 8:21 umbrella 28:13 33:2 39:16 51:16 underlying 62:6, 14 understand 10:12 17:8 35:1 37:5 41:5 47:6, 24 48:5, 15 51:10 53:5, 6, 12 56:1, 18, 22 59:19 62:6 understanding 9:4 10:14 11:11 12:15 18:6 38:1 46:25 49:8 61:23, 25 understands 34:15 50:19 58:11 unencrypted 41:12, 15, 18, 24 42:5, 16, 22 unit 49:23 UNITED 1:1 University 2:13	uploaded 14:16 21:7, 13 URI 57:21, 25 58:14 60:2, 7, 8, 16 URI/URL 57:20 URIs 58:21, 23 URL 58:6, 12 60:2, 7, 8 URLs 58:20, 23 59:10 use 42:25 44:19 56:18 59:17 66:9 uses 35:24 usually 50:14 utilizes 38:3 51:20 < V > Va 4:15 valid 34:10 variety 39:4, 17, 18 version 15:18 versus 16:24 VIDEOCONFERE NCE 1:5, 13 VIDEOGRAPHER 3:21 5:3, 17 6:4 21:9, 12 36:4, 7, 11 61:2, 5, 8 65:19 view 54:19 viewable 51:3 violations 39:2, 15 52:6, 8 virtually 7:17 virtue 31:9 visit 59:24 visiting 60:2 < W > Wacker 3:16 want 11:23 32:19 33:11	37:25 38:6 42:24 44:19 46:7 52:22 wants 46:3 Washington 2:8 way 20:18, 22 21:23 31:25 34:7 43:5 44:21 49:15 56:25 60:1 66:14 ways 39:5 42:1 45:17 53:2 web 46:3, 4, 8, 10 weigh 64:20, 21 weighed 62:4 WEISSMAN 1:6, 14 2:3 4:8 5:8 6:6, 11, 16 7:25 8:9 36:14 66:8 Welcome 61:11 well 6:14, 15 22:18, 24 28:11 29:20 31:8 34:1 39:3 40:25 47:7 48:20 52:12 58:17 well-known 44:9 well-understood 45:14 we're 7:16, 17 13:20 14:20 22:17 26:3 33:12 34:23 38:7 65:14 We've 36:1 60:23 WHEREOF 66:18 WHITE 3:21 5:4 42:23 43:7, 16 WITCOFF 3:15 5:24 within 1:16 66:6 without 64:11 WITNESS 2:3 5:13 6:5 10:7, 22 11:5 12:7 18:9 19:7, 16 20:16, 21 22:9 26:22 34:10 35:14, 24 36:3 46:7 52:12 60:11
--	--	---	--

61:1 63:21 65:13 66:13, 18 word 8:16 11:24 38:10 49:7 59:18 wording 56:11 work 9:8 15:4, 8 16:20 18:18 19:3 43:22 44:3 worked 18:23 working 10:2 15:2 17:24 45:6 65:8 worried 59:21 would 6:21 16:4, 6, 11 20:23 22:20 27:20, 25 28:24 30:6, 13, 22, 23 31:25 32:9, 23 34:2 35:2 37:5, 6, 7 39:20 40:19 41:23, 25 42:10 44:5, 17, 20, 23 45:8, 9 47:2, 5, 19 48:3, 4, 10, 11, 13, 17, 19, 22 49:18 50:2 51:1, 2, 17 52:24 53:3, 19, 22 54:4, 20 55:12 58:4 59:19 60:3 61:13 64:5 65:3, 5 wouldn't 9:14 42:18 65:4 write 8:9 < Y > Yeah 25:7 29:2 33:20 37:21 43:3 46:1 51:12 53:7 59:5 63:2 years 19:20 Yep 29:12 Yes 5:15, 16 6:18, 25 7:6 8:11 9:19 10:15 11:9 13:24 15:21, 23 17:18	21:3, 25 25:18 36:9, 10 41:13 43:14, 20 45:2 52:14 54:9 61:22 York 3:6 59:24 < Z > Zoom 5:12		
---	--	--	--