

Page 2 1 DEPOSITION OF DR. MARK MAHON, a witness, 2 called by the Patent Owner for examination, in 3 accordance with the Federal Rules of Civil 4 Procedure, taken by and before Anna Cillo, a Court 5 Reporter and Notary Public in and for the 6 Commonwealth of Pennsylvania, at the Penn Stater, 7 Hotel & Conference Center, 215 Innovation Boulevard, 8 State College, Pennsylvania, on Wednesday, February 9 12, 2025, commencing at 8:58 a.m. 10 ----- 11 APPEARANCES: 12 13 FOR THE Petitioner: 14 John Rhine, Esq. 15 john.rhine@kirkland.com 16 KIRKLAND & ELLIS LLP 17 1301 Pennsylvania Avenue, N.W. 18 Washington, D.C. 20004 19 202-389-5000 20 21 FOR THE PATENT OWNER: 22 Joseph Micheli, Esq. 23 jmmicheli@mckoolsmith.com 24 MCKOOL SMITH 25 300 Crescent Court Suite 1200 Dallas, TX 75201 214-978-4000	Page 4 1 EXHIBIT INDEX 2 3 MAR 4 PREVIOUSLY MARKED 5 2006 Curriculum Vitae, Dr. Mark P. Mahon 6 6 2005 Declaration of Dr. Mark Mahon, U.S. 10 Patent No. 10,425,817 7 8 1001 U.S. Patent No. 10,425,817 31 9 10 1004 U.S. Patent Application Publication, 33 Nair et al. 11 1006 U.S. Patent No. 8,005,219 47 12 1005 U.S. Patent Application Publication 65 Forsberg et al. 13 14 1007 3GPP TR 33.899 V1.1.0 82 15 16 1008 Nair Provisional Application 108 17 18 19 20 21 22 23 24 25 (All exhibits retained by counsel.)
Page 3 1 EXAMINATION INDEX 2 3 DR. MARK MAHON 4 BY MR. RHINE 5 5 CROSS BY MR. MICHELI 105 6 REDIRECT BY MR. RHINE 108 7 8 CERTIFICATE OF COURT REPORTER ----- 113 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Page 5 1 ----- 2 PROCEEDINGS 3 ----- 4 MR. RHINE: John Rhine for 5 petitioner, Lenovo. 6 MR. MICHELI: Joseph Micheli, with 7 McKool Smith for patent owner, Ericsson. 8 ----- 9 DR. MARK MAHON, 10 having been duly sworn, 11 was examined and testified as follows: 12 ----- 13 EXAMINATION 14 ----- 15 BY MR. RHINE: 16 Q. Good morning. 17 A. Good morning, sir. 18 Q. Can you please state your full name for the 19 record? 20 A. Yes. Mark Mahon. M-A-H-O-N. 21 Q. I'm going to go over a little bit of the 22 ground rules to help the deposition go forward 23 today. If you don't understand a question, 24 can you please tell me, otherwise I will 25 assume you've heard it and understood it?

2 (Pages 2 to 5)

Page 6 1 A. Yes. 2 Q. Can you please answer verbally so the court 3 reporter can take down your answer? 4 A. Yes. 5 Q. Please try to let me finish my question before 6 answering, and I'll try to let you finish you 7 your answer before asking my next question. 8 A. Understood. 9 Q. If you need a break, let me know. But please 10 respond to any pending question before you 11 break. 12 A. Will do. 13 Q. Is there reason today you can't give complete 14 and accurate testimony? 15 A. No, there is not. 16 Q. And you're appearing here today as an expert 17 for patent owner Ericsson, correct? 18 A. That is correct. 19 MR. RHINE: I'm going to introduce 20 what's been previously marked as Exhibit No. 21 2006. 22 - - - - 23 (Exhibit No. 2006 was previously marked for 24 identification.) 25 - - - -	Page 8 1 that work was focused on dealing security 2 aspects with those communication protocols. 3 Q. Were you involved in the development of the 5G 4 standard? 5 A. I did not attend any 3G PP working group 6 meetings. 7 Q. Have you any of the 3G PP working group 8 meetings for any of the 3G PP standards? 9 A. I have not. As part of my work -- my research 10 work, mainly funded by the DOD, I had asked 11 for permission from my sponsors to go to 12 working group meetings. And they said due to 13 my is security clearance and the work I was 14 doing, they would not permit me to do that, so 15 I did not attend. 16 Q. Have you ever developed a product for a 5G 17 network? 18 A. Commercial product, you're asking? 19 Q. We'll start with a commercial products, yes. 20 A. No, I have not. 21 Q. Have you developed a research for the 5G 22 network? 23 A. I work with graduate students doing research 24 in areas of MYMO technology, for example, as 25 well as other signaling protocols and security
Page 7 1 BY MR. RHINE: 2 Q. Dr. Mahon, this is your CV, correct? 3 A. Yes, it is. 4 Q. Is everything up to date? 5 A. Yes, it appears to be. 6 Q. What are you an expert in? 7 A. General wireless communication systems, 8 including security. 9 Q. Do you consider yourself an expert in 10 telecommunications? 11 A. I do. 12 Q. Do you consider yourself an expert in 5G? 13 A. I do. 14 Q. How did you acquire your expertise with 5G? 15 A. It began about 30 years ago when I started 16 working in the telecommunications area, and as 17 I mentioned, specifically wireless 18 communication. And my work began with the 19 first generation protocols and progressed up 20 through the second, third, fourth, and fifth 21 generation protocols. 22 I spent several decades doing research 23 specifically focused on cellular 24 communications, for example, as well as other 25 wireless communication protocols. And much of	Page 9 1 aspects associated with 5G. So we're doing 2 research in the 5G area. 3 Q. What would you say is your most relevant 4 experience to the technology at issue with the 5 '817 patent? 6 A. My decades of experience associated with the 7 understanding of how the security protocols 8 are implemented specifically with cellular 9 communications in this case, and understanding 10 and actually doing research in that area 11 through the various generations leading up to 12 the fifth generation protocol. 13 So I have intimate knowledge of how the 14 security techniques were implemented, the 15 algorithms used, and specifically at the 16 layers, one, two, three, and four, them being 17 implemented in the cellular communication 18 system. 19 Q. Before this case or any other related cases 20 had you ever heard of a SUCI? 21 - - - - 22 (Court reporter clarification.) 23 - - - - 24 MR. RHINE: SUCI, S-U-C-I. 25 THE WITNESS: I pronounce it SUCI.

3 (Pages 6 to 9)

Page 10	Page 12
1 A. I don't recall when the first time I heard the 2 acronym SUCI. So I wouldn't be able to give 3 you an exact date. Whether it predates my 4 involvement in this case, I -- I just don't 5 recall. Certainly the term has been around, I 6 -- I just don't remember when I heard it. 7 - - - - 8 (Exhibit No. 2005 was previously marked for 9 identification.) 10 - - - - 11 MR. RHINE: Going to introduce what 12 is previously marked as Exhibit No. 2005. 13 BY MR. RHINE: 14 Q. Dr. Mahon, this is your declaration in this 15 IPR, correct? 16 A. Yes, it is. 17 Q. And is this declaration accurate as you sit 18 here today? 19 A. Are you asking me if I know of any typos or 20 mistakes that I'd like to correct? 21 Q. (Indicating.) 22 A. There are not that I can think of. 23 Q. Okay. When was the first time you saw a draft 24 of your declaration? 25 A. I produced a draft at some point, and working	1 A. Not that I can recall, no. 2 Q. All right. I'd like to discuss your 3 preparation for today's deposition. Did you 4 meet with counsel to prepare for your 5 deposition today? 6 A. Yes, I did. 7 Q. And how long did you meet with counsel to 8 prepare for today's deposition? 9 A. I met approximately two or three hours on 10 Monday, and about four, four and a half hours 11 yesterday. 12 Q. And aside from Ericsson's attorneys was anyone 13 else present the days you spent preparing to 14 testify today? 15 A. No. 16 Q. Did you meet with any other experts working 17 for Ericsson in this IPR? 18 A. No, I did not. 19 Q. And do you feel sufficiently prepared to give 20 your deposition today? 21 A. I do. 22 Q. So I'd like to talk about the '817 patent and 23 as mentioned, can we first start -- let me ask 24 you a question. 25 What is your -- what in your opinion is
Page 11	Page 13
1 with Counsel, I don't recall when that was. 2 It was last fall some time. But I don't 3 remember exactly when. 4 Q. And what did you do to prepare your 5 declaration? 6 A. Well, I read through the relevant documents, 7 obviously the patents, I read through Dr. Bims 8 report, reviewed the prior art that was cited, 9 as well as other documents put forward by the 10 PTAB, and the -- the original as I have listed 11 here in my declaration, Dr. Bims' ITC 12 deposition, I read through the staff's post- 13 hearing brief, obviously Lenovo's petition for 14 the IPR, and Ericsson's documents, such as 15 their patent owner's preliminary response. 16 Q. What is the relevance of staff post-hearing 17 brief? 18 A. It was providing me with context of how the 19 staff understood my IDC deposition testimony. 20 Q. Other than your attorneys did you meet with 21 anybody else in preparing this declaration? 22 A. No, I did not. 23 Q. And did you review any documents that aren't 24 cited here in paragraph 20 of your 25 declaration?	1 novel about the '817 patent's alleged 2 invention? 3 A. Well, the novelty of the '817 is focused on 4 their disclosure of a technique, an 5 architecture, and methodology for protecting 6 the users permanent identifier. And they came 7 up with a construct they called a SUCI, and 8 that SUCI has specific elements in it, a clear 9 text part and an encrypted part and also 10 particular fields that are important for 11 permitting the protection of the permanent 12 identifier to work within the control plane of 13 the communications network, and permits the 14 protection of that identifier not only across 15 the air interface but also within a visiting 16 network to the point where it's sent to the 17 home network for deconcealing. 18 And this solved a problem that existed 19 for decades, well known in the 20 telecommunications industry, which was the 21 exposure of a user's identifier which can be 22 intercepted and used for nefarious purposes. 23 And there had been previous techniques that 24 were attempted to be implemented to be able to 25 protect that identifier, but were unsuccessful

4 (Pages 10 to 13)

Page 14	Page 16
1 and vulnerable to attacks. 2 But their solution that they came up with 3 and they coined the term, the acronym SUCI, as 4 part of that invention to protect that 5 identifier, solved the majority of the 6 problems and also greatly protected -- 7 provided great protection for the -- the 8 user's identifier. 9 Q. Which fields of the SUCI -- or the SUCI are 10 invented? 11 A. Well it's the entire aspect of the SUCI that's 12 invented, it's how they put it together. 13 Obviously providing for the ability to encrypt 14 the SUCI -- or the SUPI, I'm sorry, which is 15 S-U-P-I -- to protect it, as well as providing 16 the encryption scheme identifier, as well as 17 providing the public key identifier, to allow 18 the flexibility of the user device and the 19 network to accommodate various encryption 20 schemes as well as protect the SUCI and have 21 the ability to inter-operate within the modern 22 communications system, the 5G network. 23 Q. Was an encrypted SUPI novel at the time of the 24 invention of the '817 patent? 25 A. In the past certainly it was known that if you	1 A. It was known to protect the permanent 2 identifier, you could encrypt it, yes. 3 Q. Were encryption scheme identifiers known in 4 the art prior to the '817 patent? 5 A. The '817 discloses an encryption scheme 6 identifier, and within the context how it's 7 identified in the '817, it was not known in 8 the prior art. 9 Q. What do you mean by, "in the context of the 10 '817 patent?" 11 A. As I mentioned, there's a construct for the 12 SUCI that's disclosed in the '817 and how it 13 is communicated to the network and what 14 network elements are involved. 15 And that is, as I mentioned before, part 16 of the novelty associated with the '817, and 17 is part of the claim elements. They 18 specifically have used the term the 19 "encryption scheme identifier" within that 20 context. So that's -- that's what I'm 21 referring to. 22 Q. So the use of an encryption scheme identifier 23 in a SUCI is novel in your opinion? 24 A. It's the entire disclosure within the four 25 corners of the '817 patent that's novel and
Page 15	Page 17
1 want to protect the IMSI, which is the 2 International Mobile Subscriber Identifier, 3 you'd want to protect it in some fashion. 4 One way is to provide a temporary 5 identifier, but the problem with the temporary 6 identifier is you're still exposing the IMSI 7 at some point in time, so there were proposals 8 to encrypt the IMSI, so that was known. 9 Q. And an IMSI is a SUPI, correct? 10 A. The IMSI and the SUPI, as disclosed in the 11 '817 and used up to the point -- that point in 12 time, they're -- contained -- they contained 13 the same information. 14 There was a new acronym applied to it 15 because of the fact that, how it was being 16 used in the new generation system, and 17 specifically with the integration of 18 encrypting it into the SUCI, but the contents 19 are -- are the same. 20 Q. So in the context of the '817 patent the IMSI 21 is an example of a SUPI? 22 A. The IMSI would be considered a globally unique 23 platform and identifier. 24 Q. If -- you would agree that an encrypted SUPI 25 was known in the art prior to the '817 patent?	1 how it's integrated into that disclosure, 2 that's the novel part. 3 Q. But an encryption scheme identifier in general 4 was known before the '817 patent? 5 A. There were other ways -- there were various 6 mechanisms for identifying encryption schemes, 7 but not -- not in the way that the encryption 8 scheme identifier was used in the '817. That 9 term, again, as part of the claim elements, 10 was not known in the prior art. 11 Q. An encryption scheme identifier could just be 12 a number that represents an encryption scheme, 13 correct? 14 A. There certainly are multiple ways to identify 15 an encryption scheme, whether it's a value, a 16 string, there's various ways to do it. 17 Q. The claims of the '817 patent don't require 18 any particular format of the encryption scheme 19 identifier? 20 A. The '817 actually discloses multiple ways, 21 including strings as I mentioned -- a string, 22 several bits, so they actually disclose 23 multiple ways of -- of representing the 24 encryption scheme identifier. 25 Q. So what is particularly novel about the way

5 (Pages 14 to 17)

Page 18	Page 20
1 the SUCI uses an encryption scheme identifier? 2 A. Well it's how it's encompassed within the SUCI 3 and passed through the network for the 4 protection of the permanent identifier, and 5 then how it's anchored to the home network. 6 And so the novelty, again, as I mentioned was 7 solving the problem which existed for decades, 8 that people were trying to -- had made various 9 attempts to solve. 10 And the novelty again is how they put 11 that together within the SUCI and how the 12 network elements, such as the authentication 13 server and the SIDF, come into play and where 14 they're located within the home network and 15 the visiting network or roaming network that 16 allows -- that provided them with a solution 17 that nobody else had provided before. 18 And as I said, there were various 19 attempts that were trying to solve the same 20 problem that were unsuccessful. 21 Q. What in particular about the encryption scheme 22 identifier in the SUCI allowed it to solve the 23 solution that nobody had previously solved? 24 A. It was the understanding of the, in my view, a 25 person of ordinary skill in the art would	1 transmitted containing the SUCI and the SIDF, 2 based upon the encryption scheme that is -- 3 was used to encode the permanent identifier. 4 Q. Is the alleged novelty that you can use more 5 than one type of encryption scheme? 6 A. Well it provided the flexibility, that's part 7 of the novelty. It provided the flexibility 8 with our changing communication systems to 9 provide for the flexibility of integrating in 10 new encryption schemes as they were being 11 rolled out or as they changed or as the 12 requirements for the network operator decided 13 that they want to implement a new technique. 14 So that flexibility is integrated in to their 15 novel design. 16 Q. What about the public key identifier is novel? 17 A. About a public key identifier? 18 Q. Sure. 19 A. Public key identifier is a term that's been -- 20 that is used -- specifically within '817 -- is 21 used to enable the system, again, to provide 22 flexibility for handling different 23 public/private key pairs. 24 And by providing an identifier within the 25 SUCI, it allows, again, the system to flexibly
Page 19	Page 21
1 understand, that was their view and 2 understanding of how the 5G architecture 3 should be used and integrated in with their 4 inventive disclosure of the SUCI and putting 5 those elements together along with their 6 understanding of the architecture and how it 7 should be handled through the processing 8 elements in the architecture. 9 Q. Did the '817 patent invent an authentication 10 server? 11 A. The '817 patent calls out an authentication 12 server, certainly the term "authentication 13 server" was known prior to the '817. 14 Q. And was the term "decryption server" known 15 prior to the '817 patent? 16 A. Again, in terms of performing encryption and 17 decryption, using the term decryption server 18 outside of the context of what the '817 was 19 disclosing was no. 20 Q. What about the 5G architecture is novel in 21 with regard to what it does with the 22 encryption scheme identifier? 23 A. The '817 discloses using an authentication 24 function to be able to select, based upon the 25 contents of the messages that's been	1 react to different public/private key pairs 2 being used by devices and network operators, 3 so that even if it's a roaming context at 4 the -- the decryption can be handled by the 5 home network and the reach back can handle -- 6 be handled efficiently while protecting the 7 user's permanent identifier. 8 Q. And public key identifiers were (inaudible) -- 9 ---- 10 (Court reporter clarification.) 11 ---- 12 MR. RHINE: Sure. I'll just ask the 13 question again. 14 BY MR. RHINE: 15 Q. Public key identifiers were known in the art 16 prior to the '817 patent, correct? 17 A. Public key identifiers were known in the prior 18 art. 19 Q. In prior art public key identifiers identified 20 one of multiple public keys used for 21 encryption and decryption, correct? 22 A. Public key identifier as it was used in the 23 prior art would be used to identify a 24 particular public key associated with an 25 encryption scheme, in that context, yes.

6 (Pages 18 to 21)

Page 22	Page 24
1 Q. Is the way the '817 patent uses the public key 2 identifier different than how a public key 3 identifier was used in the prior art? 4 A. Yes. 5 Q. How? 6 A. The way it's integrated into the SUCI and the 7 in conjunction with the encryption scheme 8 identifier, and again, how it's handled by the 9 network, that was novel, yes. 10 Q. So the idea of putting them all in together 11 into one overall package, the SUCI, is the 12 inventive feature? 13 A. How it is disclosed in the '817, that the 14 entire SUCI as well as, as I mentioned before, 15 how the message is handled -- intended to be 16 handled by the network -- to permit the 17 network to be able to protect that permanent 18 identifier until it gets back into the home 19 network for decryption, that entire package as 20 well as the disclosed techniques are invented. 21 Q. What is your opinion is a technical field of 22 the '817 patent? 23 A. It's protecting privacy and protection during 24 the authentication process for a 25 telecommunication system, wireless network.	1 A. It's data associated with the user's 2 identifier. 3 Q. At the time of the invention of the '817 4 patent would a person of ordinary skill in the 5 art be motivated to achieve secure, efficient 6 data exchange? 7 A. I'm not sure I understand your question. 8 Q. Would a person of ordinary skill in the art, 9 at the time of the invention of the '817 10 patent, find secure and efficient data 11 exchange to be a beneficial future of a 12 telecommunication system? 13 A. Yes. 14 Q. In the '817 patent one of the encryption 15 schemes that can be indicated by the 16 encryption scheme identifier is the null 17 encryption scheme, correct? 18 A. That is correct. 19 Q. Null encryption doesn't use a public key, 20 correct? 21 A. Null encryption, as the POSITA would 22 understand, doesn't encrypt, so there's no 23 need for a public key. 24 Q. When the null -- in the context of the '817 25 patent -- when the null scheme is indicated,
Page 23	Page 25
1 Q. Are 4G and 5G networks different fields 2 invention? 3 A. It would depend upon the particular technical 4 issue you're looking at. It could be. 5 Q. Would you look -- if you were interested in a 6 5G network, would you consider looking at 7 prior art from 4G networks? 8 A. I think you would be informed about the 9 security techniques within 4G if you're 10 interested in applying something to 5G, yes. 11 Q. 5G systems can be used for internet access, 12 right? 13 A. For internet access? There's a control plane 14 and data plane in the 5G network that you can 15 use to connect to the internet. 16 Q. And 5G networks can be used for voice calls, 17 right? 18 A. Since the beginning of -- of wireless 19 networks, you could use -- you can use 20 wireless -- cellular networks for making voice 21 calls, yes. 22 Q. Okay. And a SUPI is data, correct? 23 A. A SUPI is a permanent identifier of the user 24 which is made of a string of bits. 25 Q. And so it is data?	1 does the SUCI still include a public key 2 identifier? 3 A. The SUCI field could still be present, but it 4 doesn't need to contain a public key 5 identifier in that case. 6 Q. Would it still include the public key 7 identifier field? 8 A. It -- the SUCI, that field would be beyond the 9 context of the -- how the user and our network 10 would warrant that field to be populated. It 11 could be present but it would be zeroed out, 12 most likely. 13 Q. The '817 patent didn't invent the concept of 14 encrypting messages in cellular 15 communications, correct? 16 A. Encryption techniques, including messages -- 17 control message encryption was known and used 18 in prior networks. 19 Q. And the concept of encrypting some portion of 20 messages and keeping other portions 21 unencrypted wasn't something the '817 patent 22 invented, right? 23 A. What context of the network protocol are you 24 thinking about? 25 Q. Any context.

7 (Pages 22 to 25)

Page 26	Page 28
1 A. So whether it's control plane, data plane, 2 certainly message structures, you have header 3 fields, for example, that are not encrypted 4 and then you can have encrypted parts of those 5 messages being transmitted. 6 Q. The '817 patent didn't invent elliptic curve 7 integrated encryption scheme, did it? 8 A. It did not. 9 Q. What is the benefit of the elliptic curve 10 integrated encryption scheme? 11 A. Well, it's a technique that uses an elliptic 12 curve for being able to generate a -- 13 encryption -- particular integrated encryption 14 scheme that is very hard to break, meaning you 15 would have to put in a lot of computational 16 resources to try to figure out what particular 17 points on the elliptic curve were used to do 18 the encryption. 19 So it provides for a mechanism for 20 basically efficiently implementing an 21 encryption with respect to how strong the 22 encryption scheme is. And also it's very hard 23 to take the information that's being passed, 24 to break the encryption scheme, which is 25 obviously a desirable technique for encryption	1 that indicated when ECIES was first proposed 2 to 3G PP as part of a possible encryption 3 scheme solutions. 4 Q. I'd like to talk about some of the opinions 5 you provided in this IPR. 6 In your opinion an encryption scheme 7 identifier must identify two or more potential 8 encryption schemes, correct? 9 A. That's correct. 10 Q. And as we already discussed, one example of an 11 encryption scheme in the '817 patent is the 12 null scheme, right? 13 A. The '817 patent does disclose the null scheme, 14 yes. 15 Q. And another example is ECIES? 16 A. That is correct. 17 Q. Do you mind turning to paragraph 55 of your 18 declaration, Exhibit No. 2005? 19 A. Okay. I'm there. 20 Q. In the footnote one at the bottom here, and in 21 the context of paragraph 55, you say that a 22 4-bit identifier would be able to identify 16 23 possibilities, correct? 24 A. That's correct. 25 Q. And you would agree that a 2-bit identifier
Page 27	Page 29
1 schemes to have, or characteristic I should 2 say for those to have. 3 Q. Did the inventors of the '817 patent suggest 4 using (inaudible) -- 5 ---- 6 (Court reporter clarification.) 7 ---- 8 9 MR. RHINE: Let me revise the 10 question. 11 BY MR. RHINE: 12 Q. Did the inventors of the '817 patent -- strike 13 that. Third time is the charm hopefully. 14 Were the inventors of the '817 patent the 15 first to propose using elliptic curve 16 integrated encryption in a 5G network? 17 A. I don't recall -- I don't recall prior art 18 citing that, but I can't say for sure that 19 they are the first. 20 Q. Do you know if Ericsson proposed adding ECIES 21 to the 5G standard? 22 A. I don't know. Again, I can't recall when the 23 suggestion, other than seeing Ericsson's prior 24 documents in the IPT case, discussing their 25 proposals to 3G PP of seeing any prior art	1 would be able to identify four possibilities? 2 A. Yes, it would. 3 Q. Could we go to paragraph 56 on the next page? 4 A. Yes. 5 Q. Here you state the commonality among the data 6 structures is that they all are -- are all 7 more than one bit, and can therefore represent 8 more than two states, do you see that? 9 A. Yes, I do. 10 Q. It's your understanding that the encryption 11 scheme identifier must have two or more 12 encryption schemes, and that understanding is 13 based on examples in the specification of the 14 '817 patent, correct? 15 A. It's based on my entire reading of the '817 16 patent, yes. 17 Q. The '817 patent never expressly defines an 18 encryption scheme identifier as having the 19 capability of two or more possible values, 20 correct? 21 A. I disagree with that. 22 Q. Okay. Where in the '817 patent does it 23 expressly require two or more possible values? 24 A. Throughout the disclosure of the '817 patent, 25 POSITA would understand that the whole intent

8 (Pages 26 to 29)

Page 30	Page 32
1 and purpose is to provide the flexibility, 2 including what we just cited in my paragraph 3 55, that the discussion and the disclosure 4 support, a clear understanding that the system 5 is designed to handle more than two encryption 6 schemes. 7 Q. Can we go just above paragraph 50 in your 8 declaration? 9 A. Yes. 10 Q. You have Figure 3 from the '817 patent 11 identified here, correct? 12 A. Yes, I do. 13 Q. And this is example in the SUCI? 14 A. Yes, it is. 15 Q. It shows an encryption scheme identifier, 16 correct? 17 A. Yes, it does. 18 Q. Figure 3 doesn't show how many possible values 19 there are for that encryption scheme 20 identifier, does it? 21 A. Figure 3 is a high level sketch of the 22 construct of the SUCI. 23 Q. It doesn't show how many possible values there 24 are for that encryption scheme identifier, 25 correct?	1 values for the encryption scheme identifier, 2 correct? 3 A. Yes, it does. 4 Q. The value of zero indicates the null scheme, 5 correct? 6 A. Yes, it does. 7 Q. And the SUCI doesn't use the word "null 8 scheme," right, it uses the value of zero? 9 A. In terms of the indication of what can be 10 contained in the -- it does disclose -- the 11 '817 discloses you could use a string. So 12 technically you could put that in there, but 13 as illustrated on this document, it's 14 indicating to use a value of zero for the null 15 scheme. 16 Q. Okay. And the value of one indicates ECIES, 17 correct? 18 A. Yes, it does. 19 Q. How does the UE know that one means ECIES? 20 A. Well that would be based upon the protocol, 21 that is the 5G protocol, indicating what each 22 one of those values would be -- how those 23 would be related to the multiple possible 24 encryption schemes can be utilized by the 25 user device -- user device.
Page 31	Page 33
1 A. It doesn't indicate any limitation associated 2 with the contents of the encrypted scheme 3 identifier. 4 MR. RHINE: I'm going to introduce 5 Exhibit No. 1001, this is the '817 patent. 6 ---- 7 (Exhibit No. 1001 was previously marked for 8 identification.) 9 ---- 10 BY MR. RHINE: 11 Q. Dr. Mahon, do you mind turning to Figure 4 12 please? 13 A. Yes, I will. Okay, I'm there. 14 Q. And this figure also has an encryption scheme 15 identifier, correct? 16 A. Yes, it does. 17 Q. After it uses the word "encryption scheme 18 identifier," it uses E, period, G, period, 19 correct? 20 A. Yes, it does. 21 Q. And you understand that is an example of an 22 encryption scheme identifier? 23 A. That is listing examples of the encryption 24 scheme identifier, yes. 25 Q. Okay. So this figure gives some exemplary	1 Q. And how does the decryption server know that 2 one means ECIES? 3 A. It would be based, again, upon the protocol. 4 Q. Do the UE and the encryption server have to be 5 on the same page to have the same 6 understanding of value? 7 A. They would have to be using the values that 8 correspond to the correct encryption scheme 9 protocols. 10 Q. There's no third example of an encryption 11 scheme in Figure 4, correct? 12 A. There is. There's the ETC, meaning "et 13 cetera," indicates to a POSITA that there's 14 other encryption schemes there -- referenced 15 there. 16 Q. That there are other encryption schemes or 17 there could be other encryption schemes? 18 A. Well, in this case et cetera meaning there -- 19 you could include other encryption schemes. 20 It's not -- again, that doc -- that figure is 21 not limiting it to a certain number. 22 ---- 23 (Exhibit No. 1004 was previously marked for 24 identification.) 25 ----

9 (Pages 30 to 33)

Page 34	Page 36
1 MR. RHINE: Going to introduce 2 what's been previously marked as Exhibit No. 3 1004. 4 BY MR. RHINE: 5 Q. Dr. Mahon, in Nair, encryption scheme that's 6 used requires both a private key and a public 7 key, correct? 8 A. The disclosure is associated with using a 9 single public and private key pair. 10 Q. A key pair is two keys, correct? 11 A. A -- well, you have two separate keys, and if 12 you're counting one plus one that would be 13 two. 14 Q. Okay. Do you mind turning to Paragraph 38 of 15 Nair? 16 A. Okay, I'm there. 17 Q. In your opinion this paragraph in Nair teaches 18 an each SLF has one and only one public key, 19 correct? 20 A. The disclosure in Paragraph 38 as understood 21 by a POSITA within the context of Nair would 22 understand that the SLF would need to have the 23 public key, and it would be a single public 24 key. 25 Q. Do you mind moving forward to Paragraph 57?	1 multiple HSSs, state specifically that a 2 single SLF will be used for directing the 3 traffic to those multiple HSSs. 4 Q. If you mind turning back to Nair please, 5 Exhibit No. 1004. I'm going to district you 6 to Paragraph 11. 7 Nair relates to security and privacy 8 features for transmitting user identifiers 9 within a wireless communication system, 10 correct? 11 A. That is indicated in Paragraph 11, yes. 12 Q. And so you would agree that Nair relates to 13 the field of privacy protection for subscriber 14 identification? 15 A. Yes. 16 Q. And Nair is directed at solving the problem 17 that unencrypted mobile subscription 18 information numbers -- such as IMSIs -- can be 19 captured by third parties when they are sent 20 in clear texts, correct? 21 A. Nair is directed towards protecting the user's 22 identifier by encrypting it. 23 Q. Can we turn to Paragraph 27 of Nair? 24 A. Okay. 25 Q. Nair recognizes that the privacy and
Page 35	Page 37
1 It's on Column 5, or Page 5. 2 A. Okay. I'm there. 3 Q. Paragraph 57 explains Figure 1 of Nair only 4 illustrates a single SLF, correct? 5 A. Paragraph 57 states; Although only a single 6 UE, et cetera, SLF elements are shown in the 7 Figure 1 embodiment, this is for simplicity 8 and clarity of description only, given 9 alternative embodiment may, of course, include 10 larger numbers of such system elements. 11 So it's -- Paragraph 57 is saying that 12 the system elements in total, you can have 13 more of those elements within their network. 14 - - - - 15 (Court reporter clarification.) 16 - - - - 17 A. Network. 18 BY MR. RHINE: 19 Q. Nair thus contemplates more than one SLF, 20 correct? 21 A. Well this disclosure isn't specifically just 22 focusing on the SLF, but I don't see a 23 limitation of only having a single SLF within 24 their network but -- however, their disclosure 25 specifically dealing with the -- using	1 subscription identifiers, when communicating 2 over the air interface, is that a problem for 3 2G, 3G, and 4G networks, correct? 4 A. Yes, they are trying to solve the same 5 problem, yes. 6 Q. And Nair recognizes that efforts have been 7 made in 5G networks to identify -- to address 8 this issue? 9 A. Yes, it does state that. 10 Q. And Nair teaches using encryption to conceal a 11 UE subscription identifier during the 12 authentication process for joining new UEs to 13 a network, correct? 14 A. Nair is directed to an authentication process 15 and encrypting the IMSI as part of that 16 process. 17 - - - - 18 (Court reporter clarification). 19 - - - - 20 THE WITNESS: IMSI, I-M-S-I. 21 BY MR. RHINE: 22 Q. Can we turn to paragraph 43 in there? 23 A. I'm there. 24 Q. Nair discloses what's called a privacy 25 indicator, correct?

10 (Pages 34 to 37)

Page 38	Page 40
1 A. Yes, it does. 2 Q. And Nair also teaches that using privacy 3 indicators saves processing time and you'd use 4 fewer resources, correct? 5 A. Nair is directed to an efficient, fast method 6 of handling a user authentication request. 7 Q. And the use of privacy indicators saves 8 processing time? 9 A. That is what the Nair disclosure is about, 10 yes. 11 Q. And Nair discloses that privacy indicators 12 result in fewer resources being used, correct? 13 A. Nair's disclosure, the use of the privacy 14 indicator is specifically so that the network 15 can quickly decrypt the encrypted IMSI. 16 Q. Turning to Paragraph 50 in there? 17 A. Okay. I'm there. 18 Q. Nair discloses a UE, correct? 19 A. Yes. 20 Q. And you would expect that a UE comprises 21 processing circuitry and memory circuitry, 22 right? 23 A. Yes. 24 Q. And so you're not disputing that Nair 25 discloses a UE with processing circuitry and	1 A. Yes, I do. 2 Q. You aren't disputing that AUSF is an 3 authentication server, are you? 4 A. No. 5 Q. In Figure 6 there's also an SLF, 610, do you 6 see that? 7 A. Yes, I do. 8 Q. Are you not disputing that the SLF is a 9 deconcealing server, are you? 10 A. As disclosed in Figure 6, it does say that the 11 SLF decrypts the encrypted IMSI, so it would 12 be performing the decryption in their system. 13 Q. Is a deconcealing server any server that 14 performs decryption of an encrypted SUPI? 15 A. Within the context of the '817, the 16 deconcealing server sits in the home network 17 and is -- receives the encrypted SUPI from -- 18 is selected by the AUSF for doing the 19 deconcealing. 20 In that case, it does perform decryption 21 as -- it similarly performs decryption. 22 Q. And so you're not disputing that the SLF in 23 Figure 6 of Nair is a deconcealing server in 24 the context of the '817 patent, correct? 25 A. Well, within the disclosures of the claim is,
Page 39	Page 41
1 memory circuitry, right? 2 A. Well a POSITA would understand that, if you're 3 talking about a user device, it has to have 4 some type of circuitry involved to do the 5 transmission of the signals. 6 Q. And the same is true for memory, right, it's 7 going to have to have some memory? 8 A. That -- a POSITA would understand that, yes, a 9 user device would have some type of memory 10 associated with it. 11 Q. Sorry to keep bouncing around, do you mind 12 going to Paragraph 42. 13 A. Okay. I'm there. 14 Q. You aren't disputing that Nair discloses a 15 SUPI, correct? 16 A. I am not disputing that the -- that Nair 17 discloses the use of an IMSI, which is -- 18 what's disclosed as a SUPI, and they do use 19 the term "SUPI." 20 Q. And Nair also discloses that a UE sends the 21 IMSI in an encrypted form to an AMF, correct? 22 A. Yes, that's correct. 23 Q. If you don't mind turning to Figure 6 of Nair? 24 A. Okay. I'm there. 25 Q. Do you see element 608, the AUSF?	1 yes, because the SLF is not being selected for 2 performing the decryption based upon the 3 received message, but it certainly is 4 performing decryption in their system. 5 Q. Does Claim 1 of the '817 patent require that 6 the deconcealing server is selected based on 7 the received message? 8 A. The Claim 1 states that the authentication 9 server determines a deconcealing server to use 10 to decrypt the encrypted part of the SUCI and 11 that the authentication server sending to SUCI 12 to the deconcealing server, so as part of that 13 claim element, it's requiring specific 14 functions by the AUSF and the deconcealing 15 server being selected by the -- determined by 16 the AUSF. 17 Q. In Figure 6 of Nair, the AUSF sends an 18 encrypted IMSI to the SLF for decryption, 19 correct? 20 A. It is being send by the AUSF, transmitted to 21 the SLF as depicted in the Figure 6. 22 Q. The UE in there, it is disclosed in Figure 6, 23 transmits the encrypted IMSI to the AUSF, 24 correct? 25 A. The Figure 6 shows a signal going from the UE

11 (Pages 38 to 41)

Page 42	Page 44
1 to the AMF and then authentication request 2 going from the AMF to the AUSF carrying the 3 encrypted IMSI. 4 Q. In your opinion that is an example of the UE 5 transmitting the encrypted IMSI to the AUSF, 6 correct? 7 A. The UE is transmitting encrypting IMSI which 8 arrives at the AUSF, as depicted in this flow 9 diagram. 10 Q. In the context of the claims of the '817 11 patent, does the UE have to transmit the SUCI 12 directly from the UE to the AUSF? 13 A. The claim element requires that the UE 14 transmit to the AUSF. There's no limitation 15 in terms of how many other network elements 16 touch that message. 17 Q. Do you mind turning to Paragraph 35 in Nair? 18 A. In Nair? 19 Q. Yes, please. 20 A. Okay. I'm there. 21 Q. Sorry, I meant 41. Sorry about that. 22 A. Paragraph 41, okay. 23 Q. Nair uses the term, "identity privacy flag" in 24 Paragraph 41, do you see that? 25 A. Yes, I do.	1 Q. And a null encryption scheme is the same thing 2 as not encrypting, correct? 3 A. A POSITA would understand it's effectively the 4 same thing as not encrypting. 5 Q. And going on to the next line in Nair, it 6 says, In the null encryption scheme the input 7 equals the output, and the SUPI is 8 unencrypted. 9 Do you see that? 10 A. Yes, I do. 11 Q. Nair goes on to say that, one could interpret 12 this as the SUPI or IMSI as always encrypted. 13 Do you see that? 14 A. I do see that. 15 Q. And then Nair also says, If no privacy is 16 switched on then the null encryption is used. 17 Do you see that? 18 A. Yes, I do. 19 Q. Would a person of ordinary skill in the art 20 understand that, when the privacy indicator is 21 not switched on, the null encryption scheme is 22 used? 23 A. A POSITA would understand that, when that flag 24 is not set, that the IMSI -- the SUCI -- would 25 not be protected and therefore would not be
Page 43	Page 45
1 Q. And it says, I.E. privacy indicator, correct? 2 A. Correct. 3 Q. So in your opinion, is a privacy indicator and 4 the identity privacy flag the same thing? 5 A. Yes. 6 Q. Would a person of ordinary skill in the art 7 understand that decryption of an IMSI requires 8 knowledge of the particular encryption key 9 used to encrypt the IMSI? 10 A. Could you repeat the question, please? 11 Q. Would a person of ordinary skill in the art 12 understand that an encrypted -- that the 13 decryption of an encrypted IMSI requires 14 knowledge of the particular encryption scheme 15 used to decrypt the IMSI? 16 A. A POSITA would understand that to do 17 decryption you have to use a compatible -- 18 typically an invertible encryption scheme -- 19 so that knowledge would be required. 20 Q. Moving on to Paragraph 42, the bottom of 21 column -- the left hand column of Page 5, Nair 22 also discloses a null encryption scheme, 23 correct? 24 A. Paragraph 42 does contain the phrase null 25 encryption scheme.	1 encrypted. 2 Q. Therefore the null encryption scheme would be 3 used? 4 A. It's unencrypted, which you could -- again 5 based on the construct of a null encryption 6 scheme, meaning nothing was done to it, you 7 would understand that nothing was done to it 8 and it's not encrypted. 9 Q. Do you mind turning to Paragraph 98 of your 10 declaration? 11 A. 98 of my declaration, yes. Okay. I'm there. 12 Q. In Paragraph 98 you say that, if Nair 13 identified the encryption scheme in the SUCI, 14 a POSITA would have expected the attached 15 request to include the identifier, right? 16 A. Yes. 17 Q. Why? 18 A. Because in order to do the decryption you need 19 additional information. 20 MR. MICHELI: Mr. Ryan, we've been 21 going for an hour, if you want to take a break 22 shortly. 23 MR. RHINE: Yeah, give me one or two 24 questions, then we can take a break -- unless 25 you want to break now?

12 (Pages 42 to 45)

Page 46	Page 48
1 THE WITNESS: No, I'm fine. 2 BY MR. RHINE: 3 Q. We can turn to Paragraph 100? Your opinion as 4 stated in Paragraph 100 relies on Nair's 5 teaching that the receiving device already has 6 the private key needed for decryption, right? 7 A. Correct. 8 Q. Claim 1 requires a public key identifier for a 9 public key of the home network, right? 10 A. Correct. 11 Q. Claim 1 doesn't require a private key 12 identifier? 13 A. In the context of the transmission, the POSITA 14 would understand that a private key is 15 protected within the network, and it's only 16 the network that needs to identify that 17 private key, so it would not be included or 18 expect to be included in that transmission. 19 Q. In fact, in the context of the '817 patent, 20 you would expect the deconcealing server 21 already has the privacy key needed for 22 decryption, right? 23 A. For each encryption scheme used, yes. 24 Q. It would have to, correct? 25 A. It would need to, to be able to do the	1 networks, correct? 2 A. Togawa is oriented and teaching specifically 3 associated with voice data or multimedia data 4 in a network. 5 Q. In your opinion is the data in Togawa limited 6 to only to voice and multimedia data? 7 A. Togawa is oriented towards encryption of -- a 8 technique for encryption of voice and 9 multimedia communications in a legacy network 10 is what Togawa is oriented towards. 11 Q. Can we go to Togawa Column 3 starting at Line 12 1? Togawa discloses a technique that can be 13 used to update encryption keys and encryption 14 methods, correct? 15 A. Togawa, and specifically addressed here in 16 this column, discloses changing an encryption 17 key based on set time intervals in their 18 disclosed system. 19 Q. You don't dispute that Togawa teaches an 20 encryption scheme identifier, do you? 21 A. Togawa discloses an encrypted method 22 identifier for their system, but that's not 23 the encryption scheme identifier as disclosed 24 in the '817. 25 Q. What's the difference between an encryption
Page 47	Page 49
1 decryption. 2 MR. RHINE: Okay. We can take a 3 break please. 4 - - - - 5 (Pause in the record.) 6 - - - - 7 MR. RHINE: Okay. I'm going to 8 introduce what's been previously marked as 9 Exhibit No. 1006. 10 - - - - 11 (Exhibit No. 1006 was previously marked for 12 identification.) 13 - - - - 14 BY MR. RHINE: 15 Q. This is the Togawa reference. I would like to 16 bring your attention to Column 1 starting at 17 Line 7. Togawa's invention relates to the 18 problem of encrypting communication data and 19 communication traffic within communication 20 networks, correct? 21 A. Togawa is oriented towards encrypting data in 22 a -- a network. 23 Q. If we go to Column 2, starting at Line 29, 24 Togawa's invention also addresses the problem 25 of encrypting data within communication	1 method identifier and an encryption scheme 2 identifier? 3 A. Well the '817 discloses the encryption scheme 4 identifier as we've discussed within the 5 context of the claim elements. Within Togawa, 6 there's this set up that's being done where 7 the sender and receiver are agreeing to switch 8 keys at -- based on a given time lapse, and 9 that method, that encryption method is decided 10 as part of that control signaling in the 11 beginning, and then how often that's going to 12 change and then the encryption keys that are 13 going to be used in that exchange so there's a 14 specific order of keys that are disclosed 15 here. 16 So that method is used to determine or to 17 indicate the encryption method being used but 18 it's not the same as the encryption scheme 19 identifier and how it's used in the '817. 20 Q. You're not asserting that the difference 21 between an encryption method and an encryption 22 scheme, are you? 23 A. As general term, a method can be understood to 24 be a scheme. 25 Q. Do you mean that the encryption method

Page 50	Page 52
1 identifier in Togawa isn't part of a SUCI, is 2 that what you're trying to say? 3 A. Well, they're -- they're not oriented to teach 4 in the same areas, they're two different 5 things. Togawa is focused on, as I said, 6 voice and data communications in a -- and it's 7 oriented towards an older network, and 8 specifically for data playing transmission. 9 '817 is for authentication, which is not 10 contained in Togawa at all, and specifically 11 for authenticating the user, protecting the 12 user's identity -- which is not part of 13 Togawa -- and that the encryption scheme 14 that's disclosed -- identifier disclosed in 15 the '817 is for that purpose, which is again, 16 outside of the context of what's disclosed in 17 Togawa. 18 Q. Togawa's encryption method identifier 19 identifies the encryption scheme used to 20 encrypt data, correct? 21 A. The Togawa's encryption method is used to 22 identify what particular encryption method is 23 being used within the disclosed Togawa system. 24 Q. Togawa's encryption key and encryption method 25 identifier identify the encryption key and the	1 method for use in encryption of the user data, 2 correct? 3 A. That's correct. 4 Q. And turning back to the top of this column, 5 the encryption specification information -- I 6 don't know if I have the wrong column, sorry. 7 Pardon me. I'm sorry, lines 18 through 21. 8 The encryption specification information, 9 90, includes the information on an encryption 10 key and an encryption method ID, correct? 11 A. That's what Togawa -- Togawa states in that 12 paragraph, yes. 13 Q. Okay. Do you mind looking the same column, 14 starting Line 34? 15 A. Okay. 16 Q. Togawa teaches that the encryption scheme -- 17 sorry -- the encryption specification is used 18 so that the apparatus that exchange data can 19 be notified of the encryption scheme 20 appropriately, correct? 21 A. Those are -- that's what it states within 22 Column 23 in those lines, yes. 23 Q. Togawa teaches that sending the encryption 24 specification allows secure and efficient data 25 exchange, correct?
Page 51	Page 53
1 encryption scheme used to encrypt a 2 communicated message, correct? 3 A. Could you repeat that question? It was a 4 little long. 5 Q. Sure. Togawa's encryption key and encryption 6 method identifier, identify the encryption key 7 and the encryption scheme used to encrypt a 8 communicated message, right? 9 A. Those elements within Togawa are used to do 10 the encryption and decryption in Togawa, yes. 11 Q. Do you mind turning to -- turning back to 12 Column 23, of Togawa? 13 A. I think I'm there already. 14 Q. Give me one second, I think I lost myself. 15 A. Okay. 16 Q. If you don't mind turning to lines 17 through 17 25? 18 A. Column 23? 19 Q. Yep. Togawa teaches that its encryption 20 method identifier is the identity that 21 identifies an encryption method for use in the 22 encryption of the user data, correct? 23 A. Would you repeat the question, please? 24 Q. Sure. Togawa's encryption method identifier 25 is the identity that identifies an encryption	1 A. Yes, it does. 2 Q. Can we turn back to your declaration, 3 Paragraph 131? 4 A. Okay. I'm there. 5 Q. In Paragraph 131, you state that the purpose 6 of Nair's privacy indicator is to save time by 7 telling the HSS or SLF that encryption is 8 turned on so it doesn't waste time trying to 9 test whether encryption is used, correct? 10 A. That's correct. 11 Q. Trying to detect whether encryption is used 12 without an indicator is called "blind 13 decoding," correct? 14 A. Blinded encoding is a -- is a very broad term 15 used in communications. And in general it 16 means not being able to -- and not knowing 17 beforehand what you are trying to -- trying to 18 find is actually there. 19 Q. Okay. Is there a shorthand you could use to 20 talk about trying to detect encryption without 21 knowing the -- the particular encryption 22 scheme used? 23 A. I'm sorry, trying to detect encryption -- 24 Q. Yeah, so you said -- blind decoding is a 25 little too broad, is there a narrower term

14 (Pages 50 to 53)

Page 54	Page 56
1 that you're referring to when you're saying 2 that you can save time by not trying to detect 3 whether encryption's on or off? 4 A. Well, specifically, I'm trying to think of a 5 more narrow term that would be accurate, other 6 than an attempt to decrypt, that -- that's 7 literally what you're doing there -- 8 Q. Okay. 9 A. -- and if it works, you know it's encrypted 10 and if it's not then you know it's not. 11 Q. Okay. And it's your opinion that this 12 attempting to decrypt cannot be used if 13 there's more than one encryption option? 14 A. What I'm saying here is that in Nair it 15 discloses specifically that if you do not 16 indicate to the receiver that an IMSI has been 17 encrypted you try it -- try to decrypt it. 18 And if you're successful then you know it was 19 encrypted and if you aren't successful then 20 you can assume it's not encrypted. Or vice 21 versa, however you want to take the approach. 22 But the point of Nair is that you're 23 saying -- if you know ahead of time then 24 you're saving computational resources by not 25 having to try trial and error, you know. It's	1 encrypted or not. 2 Q. But you could, for example, try option A and 3 option B and see the which one works? 4 A. In the Nair system on the UE transmitting? 5 Q. In the context of Nair. 6 A. In the context of Nair, it discloses that you 7 could try to decrypt the message, and if 8 that's option A, or you could choose option B 9 and not try to decrypt the message, and see if 10 you can pull up the user's IMSI. But you are 11 wasting resources by doing it, that way is 12 what Nair teaches. 13 Q. And instead of wasting resources, Nair 14 discloses the use of a privacy indicator, 15 correct? 16 A. It discloses a use of a privacy indicator 17 combined with the fact that both end 18 transmitter and receiver know what encryption 19 scheme was being implemented. 20 Q. Do you mind going to Paragraph 132 on the next 21 page? 22 A. Okay. 23 Q. You say here that it is no longer impossible 24 for the SLF HSF to interpret a failed 25 encryption of the IMSI, do you see that?
Page 55	Page 57
1 probably a better term -- you don't have to 2 perform the trial and error. 3 Q. And it's your opinion that that trial and 4 error method cannot be used if there's more 5 than one encryption scheme? 6 A. It would be extra inefficient and my opinion 7 is that the whole point of Nair is efficiency 8 and speed. That's why Nair only discloses one 9 technique, and that's what I'm discussing 10 here. 11 Q. So the UE could try two different encryption 12 methods and seeing if one of the two works, 13 correct? 14 A. Well in Nair's system, there's no way for the 15 network to know unless there's an agreed -- 16 agreement ahead of time what encryption scheme 17 was used. So if the UE chose a different 18 encryption scheme, the UE wouldn't know 19 whether it was rejected because of the failure 20 to decrypt or if there was something else 21 going on preventing it from being attached, 22 which is why Nair's system is so focused on 23 making sure that the encryption is known by 24 both hands beforehand and that they have this 25 simple Boolean flag to tell it whether it's	1 A. Yes, I do. 2 Q. And you identify two possible interpretations 3 fashions of a failed decryption of an IMSI, do 4 you see that? 5 A. Yes, I do. 6 Q. Why couldn't the UE simply try the other 7 encryption scheme? 8 A. Could you give me the scenario in which this 9 is occurring the UE transmitting an 10 authentication request through the network? 11 Q. In the context you're discussing in Paragraph 12 132. 13 A. Well the UE would have to receive information 14 from the network saying that, for example, the 15 message could not be decoded due to errors, 16 bit errors or could not be decoded because of 17 some other reason determined by the network. 18 It would have to receive a message back 19 from the network to know the reason why. So 20 the UE would be basically performing blind 21 transmission. It would try to transmit using 22 encryption method A. If it doesn't work, it 23 could try A again. It could try A again. It 24 could try another one, if it wanted to. But 25 obviously that's a very inefficient

15 (Pages 54 to 57)

Page 58	Page 60
1 implementation, not what Nair is teaching 2 towards. 3 Q. The purported solution of the '817 patent 4 doesn't solve the problem identified in 5 Paragraph 132 does it? 6 A. It does, because it is communicating specific 7 information about what encryption technique 8 was used. 9 Q. If the decrypted -- the IMSI decryption in the 10 '817 patent fails, how does the UE know 11 whether the error was in the UE with the 12 message -- strike that. 13 In the '817 patent how would the 14 decryption server know that the encryption 15 scheme was chosen correctly if it received a 16 failed encryption of the IMSI? 17 A. So the context that you're stating is that the 18 device in the '817 context is -- chooses an 19 encryption scheme and transmits it to the 20 network, is that correct? 21 Q. Uh-huh. 22 A. And that the network cannot decrypt the 23 authentication request? 24 Q. Yes. 25 A. The network will transmit an error message to	1 eliminate from my answer. It just was just 2 outside of the context of what I was -- 3 thought I was asked. 4 Q. Okay. Turning back to Paragraph 131, Nair's 5 privacy indicator is an alternative to the 6 trial and error method we've been discussing, 7 correct? 8 A. Well Nair's privacy indicator is their 9 solution for implementing an efficient and 10 fast authentication procedure, that's what it 11 is. 12 Q. And so Nair is not suggesting using the trial 13 and error method, it is suggesting using the 14 privacy indicator? 15 A. It specifically calls out that, if -- the 16 inventive aspect is this Boolean indicator 17 that can tell you what encryption scheme was 18 -- that the encryption scheme was being 19 performed, and therefore you can decrypt it, 20 again, given knowledge beforehand what that 21 encryption scheme was used on both aspects. 22 That's the novel aspect. So they're 23 trying to solve the problem of wasting 24 resources by performing a trial and error. 25 Q. So Nair is suggesting not doing trial and
Page 59	Page 61
1 the user based on the request for 2 authentication. So it received a message back 3 from the network, either a rejection message 4 or an error message. 5 Q. How does the encryption server know if the 6 error was in the encrypted IMSI or the 7 encryption scheme identifier? 8 A. Well the network is going to know what 9 encryption scheme was used and it'll perform 10 the proper decryption. Now if there's some 11 bit errors that come into play, that's just 12 normal communications theory, that -- that 13 happens. 14 I do want to address something else with 15 respect to the attach and authentication 16 request within the network. There are 17 contexts when you're sending up, for example, 18 an initial attach request to the network when 19 you're first turning on your device. And 20 there are procedures and protocols that you 21 follow for determining whether you were 22 successful or not. 23 That's a much broader context and a much 24 broader discussion with respect to the 25 previous question that I wasn't trying to	1 error, correct? 2 A. They're trying to implement an efficient 3 methodology, and trying to certainly put trial 4 and error as a corner case. 5 Q. So Nair's privacy indicator is an alternative 6 to the trial and error, correct? 7 MR. MICHELI: Objection, asked and 8 answered. 9 A. I -- I don't understand the question, because 10 the privacy indicator is their solution for 11 fast and efficient authentication within the 12 network, that's what they propose. 13 BY MR. RHINE: 14 Q. Right. I guess that's what I am getting at, 15 they're not -- they're proposing using the 16 privacy indicator and they're not proposing 17 using the trial and error method, which is 18 less efficient? 19 MR. MICHELI: Same objection. 20 A. Again, they're proposing to use this privacy 21 indicator, based on the understanding that you 22 have an encryption scheme being used on both 23 ends. 24 And as part of the explanation in Nair, 25 they go into discussing the fact that what

16 (Pages 58 to 61)

Page 62	Page 64
1 this solves is telling the system that 2 encryption has been done and that you can 3 quickly look at that flag, that Boolean value, 4 and say yes, encryption's on, let's perform 5 encryption; no, encryption's not on, let's 6 just decode the message since there's -- as it 7 is, without having to do encryption. 8 It presents the case where, if you didn't 9 know that, that you would be wasting resources 10 trying to figure out whether it's encrypted or 11 not. That's the context, to my understanding 12 of Nair, from a perspective of a POSITA. 13 Q. So in the Nair before the privacy indicator is 14 used, a person of ordinary skill in the art 15 wouldn't also use the trial and error method 16 at the same time, correct? 17 A. Not if they're implementing Nair's system. 18 Q. Okay. So Nair is suggesting an alternative to 19 the trial and error. Why does it matter if 20 the trial and error method is compatible with 21 multiple encryption schemes? 22 A. Again, Nair provides a solution and you can 23 either choose to use their solution or not. 24 In terms of Nair is directed to 25 efficiency and speed, it doesn't make sense to	1 Q. So why does it matter if Nair's inferior 2 solution is incompatible with multiple 3 encryption schemes? 4 MR. MICHELI: Objection, asked and 5 answered. 6 A. What do you mean Nair's inferior solution? 7 BY MR. RHINE: 8 Q. The trial and error method? 9 A. Could you ask the question again, please? 10 Q. Why does it matter if Nair's trial and error 11 solution is incompatible with multiple 12 encryption schemes? 13 A. So for -- in this section I'm discussing the 14 motivation to combine Togawa with Nair in 15 Forsberg, so I'm pointing that out for a lack 16 of motivation to combine, that's why it 17 matters. 18 Q. Is Dr. Bims relying on the trial and error 19 method disclosed in Nair as disclosing the 20 encryption scheme identifier? 21 A. My recollection is Dr. Bims provides scant, if 22 any, motivation to combine. 23 Q. You don't dispute that Nair and Togawa are in 24 the same field of invention, do you? 25 A. I dispute that Nair and Togawa are -- a person
Page 63	Page 65
1 use the trial and error method to handle 2 multiple encryption schemes, it's just 3 incompatible what Nair's -- teaches to. 4 Q. Okay. So in Paragraph 32, why are you 5 pointing out that it would no longer be 6 possible for the SLF HSF to interpret a failed 7 encryption -- 8 A. Because of the ambiguity if you tried to do 9 that. Again, it goes against what Nair is 10 teaching. 11 So suddenly, you're saying that I'm going 12 to integrate this one possibility into Nair, 13 which is incompatible with Nair, and I am 14 pointing out the incompatible -- one possible 15 -- one reason why it's incompatible with Nair, 16 you wouldn't be able to know why you failed. 17 Q. But Nair is teaching not to do the trial and 18 error decoding, correct? 19 A. Nair is trying to solve the problem of fast 20 and efficient communication and it mentions 21 trial and error as a waste of resources. 22 So their solution is to implement the 23 flag, and if you choose not to implement the 24 flag as discussed in Nair, then you will be 25 wasting resources by doing a trial and error.	1 of ordinary skill in the art would look at 2 those two as being in the same area given that 3 the '817 is focused on authentication within a 4 5G network, which is control plane function. 5 Togawa is oriented towards legacy 6 networks and data plane architecture, 7 different elements touch it, so -- and there's 8 a lot of aspects of the communications and 9 setup that go on and what problems are trying 10 to be solved in authentication versus data 11 transmission. 12 So I dispute that a person of ordinary 13 skill in the art would be motivated to combine 14 those two. 15 MR. RHINE: I'm going to introduce 16 what's previously marked as Exhibit No. 1005. 17 - - - - 18 (Exhibit No. 1005 was previously marked for 19 identification.) 20 - - - - 21 BY MR. RHINE: 22 Q. Can I bring your attention Paragraph 10? 23 A. Paragraph 10? 24 Q. Yeah, please. Nair relates to the field of 25 providing cellular communications, correct?

17 (Pages 62 to 65)

Page 66	Page 68
1 A. I'm sorry, Forsberg or Nair? 2 Q. Oh, I'm sorry. I meant Forsberg, that's 3 Exhibit No. 1005. Yeah, let me rephrase my 4 question because I definitely got that wrong. 5 Forsberg relates to the field of 6 providing cellular communication? 7 A. Well, relates to a specific aspect within 8 cellular communications. 9 Q. Which aspect is that? 10 A. It's a roaming aspect where you may be roaming 11 and the roaming network cannot identify the 12 user in reaching back to the home network. 13 Q. The '817 patent also relates to roaming 14 correct? 15 A. '817 is compatible with roaming architecture, 16 yes. 17 Q. And in the '817 patent the -- is the 18 authentication server in the home network or 19 could it also be in a visited network? 20 A. The authentication server is sitting inside 21 the home network. 22 Q. Forsberg addresses security in the context of 23 two way or multi-way communication, including 24 cellular phone calls and multimedia, correct? 25 A. In Paragraph 5 it does state that, yes.	1 A. It does not have an encryption scheme 2 identifier, and it doesn't have the other 3 elements that are disclosed to support the 4 encryption scheme identifier, which fields are 5 shown in the '817 in Figures 3, 4, and 5. 6 Q. Which fields are you referring to in Figures 7 3, 4, and 5? 8 A. Well specifically there's -- '817 contemplates 9 scheme related parameters, example of public 10 key, and those scheme related parameters could 11 include, for example, for ECIES, shared 12 secrets and other information that's needed to 13 be able to do the decryption. 14 Q. In your opinion are those fields required by 15 the claims of the '817 patent? 16 A. They are encompassed but they are not 17 specifically all required. 18 Q. And so as you were discussing earlier, you 19 agree that Forsberg teaches a public key 20 identifier, correct? 21 A. Yes. 22 Q. And Forsberg's public key identifier allows 23 identification of a public key needed to 24 decrypt the encrypted IMSI when multiple keys 25 are associated by the home network, correct?
Page 67	Page 69
1 Q. If you go to Paragraph 19, Forsberg addresses 2 the problem of encrypting user data in 3 communication traffic within communication 4 networks. 5 A. Forsberg is oriented to being able to 6 authenticate a user whose identity is 7 encrypted. 8 Q. And you don't dispute that Nair and Forsberg 9 are in the same field of invention, do you? 10 A. I do not. 11 Q. Forsberg teaches encrypting messages by using 12 a public and secret key pair, as well as a key 13 identifier, correct? 14 A. Yes. 15 Q. And can we take a look at Figure 4 of 16 Forsberg? 17 A. Okay. 18 Q. Forsberg teaches an encrypted IMSI that sent 19 part of the user identity response, correct? 20 A. Correct. 21 Q. User identity response also includes a public 22 key identifier? 23 A. Yes. 24 Q. Which elements of a SUCI are missing from the 25 user identity response in Forsberg?	1 A. It allows the network to determine what the 2 proper private key would be for a coupling 3 with the public key that was used, and that 4 would be understood by a POSITA to be 5 associated with different techniques. 6 Q. And what's the purpose of the public key 7 identifier in there -- sorry, in Forsberg? 8 A. Well, the visited MME uses it to identify the 9 network or try to decrypt the encrypted IMSI. 10 And therefore, if it has the private key 11 associated with that public key, that 12 public/private key pair, it can do the 13 decryption. If it doesn't, then it has to 14 reach back to the home network as indicated, 15 for example, in Figure 4. 16 Q. And let's turn to Paragraph 55 in Forsberg. 17 A. Okay. I'm there. 18 Q. Forsberg teaches that the public key and 19 secret key pairs are identified so that the 20 correct secret key can be used to decrypt the 21 IMSI, right? 22 A. Correct. 23 Q. Okay. And Forsberg also teaches that the 24 public key can be updated or rotated, right? 25 A. Well, certainly that the public key would be

18 (Pages 66 to 69)

Page 70	Page 72
1 associated with the home network and, 2 therefore, can be updated, it would be 3 understood, yes. 4 Q. What's the benefit of updating the public key? 5 A. Well that would be up to the network operator, 6 if they want to use a different encryption 7 scheme they can update the public key, for 8 example. 9 Q. You don't dispute that Forsberg discloses a 10 SUPI, do you? 11 A. Forsberg does not use the acronym SUPI, but it 12 certainly discloses a IMSI. 13 Q. And you don't dispute that Forsberg discloses 14 a SUPI? 15 A. Well it discloses, as I said before, an IMSI 16 which would be understood to be a long term 17 permanent identifier of the user. 18 Q. And an IMSI is discussed by Forsberg consists 19 of the mobile country code, mobile network 20 code, and a mobile subscriber identification 21 number, correct? 22 A. That's correct. 23 Q. How long has 3G PP networks used an IMSI? 24 A. IMSI -- so, we're talking decades. So if you 25 -- there may be some 3G networks that are	1 A. No, it does not. 2 Q. Forsberg generates an encrypted SUPI? 3 A. Forsberg discloses an encrypted IMSI. 4 Q. And an encrypted IMSI is the SUPI, correct? 5 A. No. 6 Q. An encrypted IMSI is an example of a SUPI, 7 correct? 8 A. No. 9 Q. Why not? 10 A. Because if you encrypt the identifier, it 11 certainly falls out of the term of a SUPI. 12 Q. I see. So an encrypted IMSI is an example of 13 an encrypted SUPI? 14 A. It's an example of an encrypted IMSI, the SUPI 15 as disclosed in the '817 and as I have 16 mentioned before, that term, that acronym was 17 invented due to the -- was introduced due to 18 the inventive aspect of the SUCI. So while 19 they contain the same information, I would 20 dispute that they're the same term -- the same 21 element as disclosed in the '817. 22 Q. You aren't disputing that Forsberg discloses 23 the SUPI because it doesn't use the name 24 "SUPI," are you? 25 A. No, I'm saying that the acronym SUPI, as
Page 71	Page 73
1 still on, I think they all turned off, but -- 2 so decades. 3 Q. So that was used in 3G? 4 A. It was used in 3G. 5 Q. Was it used in 2G? 6 A. There was an identifier in 2G, to identify the 7 equipment for the network to authenticate. 8 Q. In Forsberg SUPI is a globally unique 9 identifier allocated to a subscriber, correct? 10 A. Each -- in Forsberg each user would have an 11 individual IMSI identifying the user. 12 Q. And you don't dispute that Forsberg discloses 13 a SUPI that comprises a home network 14 identifier, identifying a home network of the 15 subscriber? 16 A. Well, as I've said Forsberg discloses an IMSI, 17 which includes the home network identifier as 18 well as an MSIN. 19 Q. Forsberg also discloses that a SUPI includes a 20 description identifier identifying the 21 subscription within the home network? 22 A. The IMSI would be associated with the 23 subscription for that user in that home 24 network. 25 Q. And Forsberg's UE generates a SUCI, right?	1 disclosed in the '817, is disclosed as part of 2 the invention of the '817. 3 I'm saying that the IMSI is -- contains 4 the same information as the SUPI, but Forsberg 5 obviously isn't using that term because that 6 wasn't in use at that point in time, because 7 of the SUPI was introduced to couple it with 8 the SUCI as part of the '817 disclosure. 9 Q. Does the terminology IMSI or SUPI change your 10 opinion on whether Forsberg discloses the 11 SUPI? 12 A. I'm sorry, does the terminology? 13 Q. Are you saying that the name matters? 14 A. Well, no, I'm just trying to draw a 15 distinction between what's disclosed in 16 Forsberg, it's an encrypted IMSI, and is that 17 the same content of information that is what's 18 disclosed as a SUPI in '817, yes. 19 Q. You would agree that Forsberg discloses a 20 SUPI, yes or no? 21 A. I -- it discloses a permanent identifier, a 22 long term permanent identifier. 23 Q. Is that a yes or a no? 24 A. Within the context of what I've just said, it 25 would be a yes.

19 (Pages 70 to 73)

Page 74	Page 76
1 Q. If we go to Paragraph 19 of Forsberg? 2 A. Okay. 3 Q. Forsberg discloses an identifier containing at 4 least one encrypted part, correct? 5 A. Yes. 6 Q. In Forsberg, the home network identifier is 7 not encrypted, correct? 8 A. That's correct. 9 Q. So if we go back to Figure 4 of Forsberg, 10 looking at the user identity response, the 11 encrypted IMSI includes an encrypted portion 12 and an unencrypted portion, correct? 13 A. Forsberg discloses that that would contain the 14 home network as well as the encrypted IMSI. 15 Q. Going back to Paragraph 19, Forsberg discloses 16 using the encrypted IMSI -- sorry, strike 17 that. 18 Forsberg discloses requesting assistance 19 in decrypting its identifier from a second 20 network entity, correct? 21 A. Yes. 22 Q. You don't dispute that Forsberg discloses 23 transmitted an encrypted IMSI to an 24 authentication server for forwarding to a 25 deconcealing server, do you?	1 Q. So you don't dispute that the home MME is a 2 deconcealing server? 3 A. It's performing decryption, so you want to say 4 that that's a deconcealing server, then it's 5 the deconcealing server, in that context. 6 Q. Person of the argument is good -- sorry, 7 excuse me. 8 A person of ordinary skill in the art 9 will understand that the server that performs 10 decryption is a deconcealing server, correct? 11 A. Well, in the context of the '817 patent, it's 12 a 5G network, Forsberg is disclosed to a 4G 13 network. The home MME performs different 14 functions than an SIDF does in a 5G network. 15 They are performing the same element of 16 decryption, so in that context only would you 17 consider it -- within a 4G context -- a 18 deconcealing server. 19 But it's not the same as what a 20 deconcealing server does in total in what I -- 21 in a 5G network, nor is what an SIDF does in a 22 5G network the same as what an MME does in a 23 4G network. 24 Q. In forming your opinions in this IPR you've 25 interpreted the deconcealing server limitation
Page 75	Page 77
1 A. Forsberg does not disclose a deconcealing 2 server. It does disclose transmitting the 3 encrypted IMSI back to the home MME for 4 decryption, and that would perform the 5 function of the SIDF that's disclosed in the 6 '817, but -- so it certainly -- if it can't 7 find the -- if it can't decrypt the user, it 8 doesn't have the public/private key pair. It 9 will reach back to the home MME for doing the 10 decryption. 11 Q. The home MME in Forsberg decrypts an encrypted 12 IMSI, correct? 13 A. In the roaming situation, proposed in 14 Forsberg, yes. 15 Q. In other words it, deconceals an encrypted 16 IMSI, correct? 17 A. It will decrypt it, which would deconceal the 18 IMSI, yes. 19 Q. In the home MME in the server? 20 A. Yes, it's a server within the home network. 21 Q. But why isn't the home MME the deconcealing 22 server? 23 A. In the context of the Forsberg disclosure it 24 is performing deconcealment of and decryption 25 of the encrypted IMSI.	1 in claims of the '817 as requiring a 5G 2 network deconcealing server, correct? 3 A. I have interpreted the claim elements with 4 respect to the disclosures in the '817, which 5 is oriented towards an -- 5G architecture and 6 the elements disclosed within that 7 architecture. 8 And I guess that's the best way I can 9 answer that. 10 Q. So in the opinion -- in the -- in your 11 understanding as you apply this IPR, a 12 deconcealing server is limited to a 5G network 13 deconcealing server? 14 A. What I'm saying is, is that the disclosures in 15 the '817 are oriented towards a 5G network. 16 Is the deconcealing function when you point to 17 a 4G network or is the decryption function 18 occurring in an home MME, yes. 19 Is it what's -- is that the same function 20 that the SIDF is performing in the '817, yes. 21 And so just in that context is how I describe 22 how I did my evaluation. 23 Q. So the MME -- the home MME in Forsberg -- 24 provides the same function as the SIDF, in the 25 '817 patent, correct?

20 (Pages 74 to 77)

Page 78	Page 80
1 A. It performs the same decrypting function. 2 Q. But in your opinion the claims of the '817 3 patent require some additional functionality? 4 A. No, it just requires the decryption as far as 5 the claim elements are concerned. 6 Q. So you don't dispute that the Forsberg's home 7 MME, would be a deconcealing server in the 8 context of the '817 patent? 9 A. The '817 patent also discloses that a certain 10 order of events have to happen, but I'm not -- 11 I'm not making that claim. 12 Q. So you're not disputing that Forsberg's home 13 MME is a deconcealing server in the context of 14 the '817 patent? 15 MR. MICHELI: Objection, asked and 16 answered. 17 A. I'm not -- I'm not disputing that. 18 BY MR. RHINE: 19 Q. You're not disputing that the visited MME in 20 Forsberg is an example of an authentication 21 server in the context of the '817 patent, are 22 you? 23 A. Again, given the same caveats, I do not make 24 that dispute. 25 Q. In Forsberg, the home MME sends back an IMSI	1 investigation with regard to whether the 2 preamble is limiting, have you? 3 A. Not that I recall. 4 Q. Okay. Can we go back to Nair, please, Exhibit 5 No. 1004? 6 A. Exhibit No. 1004, hold on a second. Okay, 7 1004, I have it. 8 Q. Could you turn to Paragraph 7 of Nair? 9 A. Okay. I'm there. 10 Q. All right. In Paragraph 7 of Nair, Nair 11 incorporates by reference TR 33.899, version 12 1.1.0, correct? 13 A. Yes, it does. 14 Q. And Nair expressly incorporates TR 33.899 in 15 its entirety, as we can see, correct? 16 A. I don't see the word "entirety" included 17 there, I don't see anything specific. I 18 see -- do see TR 33.899 and the version number 19 specified. 20 Q. In the top right hand corner of Page 1 Nair 21 says, TR 33.899, incorporated by reference 22 herein in its entirety? 23 A. I do see that, yes. 24 Q. Would you agree Nair expressly incorporates TR 25 33.899, Version 1.1.0 in it's entirety,
Page 79	Page 81
1 decryption response to the visited MME, 2 correct? 3 A. Yes, it does. 4 Q. Forsberg relates to authentication of a mobile 5 device, correct? 6 A. Yes, it does. 7 Q. That's what Figure 4 is showing, the method 8 for authenticating MME in a telecommunications 9 server -- network? 10 A. Yes. 11 Q. Looking at Figure 4 of Forsberg, if the user 12 identity response included an additional field 13 identifying the encryption scheme used, would 14 satisfy Claim 1, wouldn't it? 15 MR. MICHELI: Objection, vague. 16 A. What element of Claim 1 are we talking about? 17 BY MR. RHINE: 18 Q. All elements of Claim 1. 19 A. Well, the first -- in the preamble, it's a 20 method performed by an authentication server 21 in a home network. The authentication server 22 in this Figure 4 is not in a home network, so 23 that automatically means it doesn't even meet 24 the preamble. 25 Q. You haven't provided any opinions in this	1 correct? 2 A. Yes. 3 Q. Nair also says that TR 33.899 identifies 4 subscription UE privacy as one of the most 5 important security areas to be decreased in 5G 6 networks, correct? 7 A. It states that it identifies subscription 8 privacy as one of the most important areas to 9 be addressed in 5G networks, yes. 10 Q. In turning to Paragraph 28, Nair says, TR 11 33.899 discloses several solutions to provide 12 privacy over the air interface, right? 13 A. Yes, it does state that. 14 Q. In Paragraph 30 it describes one of the 15 solutions that relates to the encryption of 16 the permanent subscription identifier of the 17 UE, right? 18 A. Yes, it does. 19 Q. In the permanent subscription identifier, the 20 UE is a SUBI, right? 21 A. Yes, it is. 22 Q. So, as Nair describes TR 33.899 describes a 23 solution regarding encryption of a SUPI, the 24 public key of the home network operator, 25 correct?

21 (Pages 78 to 81)

Page 82	Page 84
1 A. It prevents four, no, actually three solution 2 classes and the second solution class is the 3 encryption of the permanent identifier using 4 the public key of the home network. 5 Q. So you would agree that Nair explains that TR 6 33.899 provides solutions to an encrypted SUPI 7 using the public key of the home network 8 operator? 9 A. Nair discusses that, yes. 10 MR. RHINE: I'm going to introduce 11 what is previously marked as Exhibit No. 1007. 12 - - - - 13 (Exhibit No. 1007 was previously marked for 14 identification.) 15 - - - - 16 MR. RHINE: I'd like for you to turn 17 Page 376 and look at Section 5.7.4.15. 18 - - - - 19 (Court reporter clarification.) 20 - - - - 21 MR. RHINE: 5.7.4.15. 22 A. Okay. I'm there. 23 BY MR. RHINE: 24 Q. So this section of TR 33.899 discusses a 25 solution to address the key issue concealing	1 Q. A POSITA, a person of ordinary skill in the 2 art, looking for a solution for concealing a 3 permanent subscription identifier would 4 consider this section of TR 33.899, correct? 5 A. So a POSITA would be aware of what documents 6 were available, and certainly this may be a 7 document they reference. 8 Q. Can we turn to Page 378? 9 A. We're still in the same section, correct? 10 - - - - 11 (Simultaneous speaking.) 12 - - - - 13 BY MR. RHINE: 14 Q. Okay. TR 33.899 teaches that the electric 15 curve cryptography is a good choice for mobile 16 devices because of faster computation time and 17 shorter key size, do you see that? 18 A. Yes, I do. 19 Q. Do you dispute the accuracy of that statement? 20 A. No. 21 Q. Do you dispute that the 5G standard developers 22 knew that ECIES was a good choice for the 23 mobile devices before the invention of the 24 '817 patent? 25 A. No, it -- that technique was a known technique
Page 83	Page 85
1 SUPIs, correct? 2 A. This section is specifically discussing 3 encrypting the IMSI using the ECIES encryption 4 scheme. 5 Q. And it addresses a key issue of concealing a 6 SUPI, correct? 7 A. Well, it's addressing encrypting an IMSI, 8 using that particular encryption scheme. 9 Q. And you don't dispute that this section 10 addresses a key issue of concealing a SUPI by 11 providing a way to conceal the IMSI using a 12 public key encryption? 13 A. It discusses a methodology for encrypting the 14 IMSI using a particular encryption scheme. 15 Q. And TR 33.899 says that concealing permanent 16 or long term subscription identifier is a key 17 issue, correct? 18 A. Well it's well understood that that was a 19 problem, as I mentioned, over decades and it 20 does use those words, yes. 21 Q. And as you mentioned, the solution described 22 here is concealing the IMSI using public key 23 encryption based on ECIES, correct? 24 A. This section does discuss the ECIES scheme, 25 yes.	1 that would be considered as part of any 2 encryption scheme being implemented. 3 Q. And as you can see here, using ECIES to 4 encrypt a SUPI in an 5G network was already 5 proposed before the '817 patent, correct? 6 A. The date on the document is prior art. 7 Q. So you're not opining in this IPR that using 8 ECIES to encrypt a SUPI in a 5G network was 9 invented at the time of the '817 patent are 10 you? 11 A. No. 12 Q. You don't dispute that TR 33.899 teaches 13 encrypting the MSIN of the UE, do you? 14 A. While this section of the report does not 15 specifically address -- it does address the 16 MSIN. A POSITA reading this would understand 17 that encrypting the home network information 18 would not be practical. 19 Q. You're looking at Figure 5.7.4.15.2-1? 20 A. That is one of the figures in that section, 21 yes. 22 Q. And that figure shows encrypting the MSIN but 23 not encrypting MCC/MNC? 24 A. Correct. 25 MR. RHINE: Is it time for a break?

22 (Pages 82 to 85)

Page 86	Page 88
1 Does that make sense? 2 MR. MICHELI: That's good for me. 3 - - - - 4 (Pause in the record.) 5 - - - - 6 MR. RHINE: We're going to talk a 7 little bit about the system in Nair. Exhibit 8 No. 1004. 9 BY MR. RHINE: 10 Q. I'm going to direct you to Figure 6, if you 11 don't mind. 12 A. Okay. I'm at Figure 6. 13 Q. So Figure 6, we've been discussing includes an 14 SLF, correct? 15 A. Yes, it does. 16 Q. And what is an SLF in context of Nair? 17 A. Nair terms it as a server location function or 18 a subscriber location, and they have basically 19 two configurations disclosed in Nair 20 associated with the SLF. 21 Q. An SLF -- sorry, strike that. 22 You said -- you mentioned the SLF is part 23 of the -- is it part of the home network? 24 A. For Nair? Nair is -- in the context of Nair 25 it's discussing a home network.	1 Q. How does the AMF know what is the home network 2 for the UE? 3 A. The AMF's responsibility, as part of 4 understanding of POSITA, would be that it 5 would know whether the user is roaming or not 6 based on home network information provided. 7 Q. That's the MCC -- MNC? 8 A. Correct. 9 Q. Okay. And that's part of the IMSI correct? 10 A. It is part of the IMSI. 11 Q. So the AMF will look at the home network 12 identifier to figure out which network to 13 appropriately forward the message to? 14 A. It will route the message based upon that 15 information. 16 Q. And then the AUSF sends the authentication 17 request to the SLF, correct? 18 A. That's correct. 19 Q. So which SLF the authentication request is 20 sent to depends on the home network 21 identifier, correct? 22 A. It would be routed to the home network based 23 on -- or the proper network based on the MCC 24 and MNC. 25 Q. And that's how a person of ordinary skill in
Page 87	Page 89
1 Q. Okay. Maybe I should have started with this 2 first, but the AMF, that's part of the visited 3 network, right? 4 A. Nair doesn't make a distinction in its patent 5 with respect to what elements are in what, 6 home or visited network. But it certainly 7 discusses everything in the context of home 8 network and it would be reasonable to assume 9 that an AMF could be in a visited network. 10 Q. I see. So it could be either, because 11 sometimes you're roaming and sometimes you're 12 not? 13 A. Yeah. 14 Q. And how about this AUSF, that -- probably in 15 the home network, if I understand it? 16 A. In general the AUSF would be an element that 17 would be contained within the home network. 18 Q. So in Figure 6, the AMF in Nair sends the 19 authentication request to the AUSF and the 20 home network, correct? 21 A. The AUSF is shown as sending the 22 authentication request to the SLF. 23 Q. It did also go to the AUSF too, correct? It 24 first goes to the AUSF, correct? 25 A. That's correct.	1 the art would interpret Nair? 2 A. Yes. 3 Q. In a 5G network -- strike that. 4 There are multiple home networks in the 5 United States from different providers, 6 correct? 7 A. Correct. 8 Q. So in the global network there are more than 9 one SLF, correct -- each home network has its 10 own SLF is what I'm trying to get at? 11 A. Each operator's going have their own enclave 12 of home networks, which is going to be only 13 for their purposes, so yes. 14 Q. You would agree that information in -- 15 information from the UE is used to determine 16 which SLF receives the authentication request 17 in Nair? 18 A. The home network information is transmitted by 19 the UE and is used to route the message to an 20 SLF, so it's using that information. 21 Q. Can you turn to Paragraph 59 of your 22 declaration? 23 A. Yes. 24 Q. In the third sentence of Paragraph 59, I guess 25 in the second third you say, in the opinion

23 (Pages 86 to 89)

Page 90	Page 92
1 the '817 patent is non-obvious due to it's 2 adoption in the 5G standard, which reflects 3 the 3GPP valuable contributions to 4 telecommunications security. Next generation 5 5G networks continue to be broadly deployed by 6 carriers for the U.S., I'm paraphrasing, 7 obviously, do you see that? 8 A. Yes, I do. 9 Q. So you're relying on for the evidence of the 10 non-obviousness of the '817 patent, you're 11 relying on adoption of the 5G standard, 12 correct? 13 A. I do cite to the 5G standard as an -- adoption 14 as -- as specific support. 15 Q. In your opinion is every design choice adopted 16 by the 5G standard non-obvious? 17 A. No, it depends upon the context. 18 Q. Do you know how many patents are essential to 19 the 5G standard? 20 A. Vague ideas, but, no, I do not know the exact 21 number. 22 Q. The number is in the thousands, correct? 23 A. Correct. 24 Q. Without getting into confidential information, 25 do you know how many Ericsson patents are	1 be the only way to really tell. 2 Q. So why is adoption in the 5G standard evidence 3 of non-obviousness? 4 A. Well, because they are competing ideas and -- 5 over the decades of not providing solutions, 6 that their solution was adopted, and that is 7 based on my understanding of -- and 8 experience -- that is evidence of 9 non-obviousness. 10 Q. You don't dispute that Togawa teaches using 11 multiple encryption schemes, correct? 12 A. Togawa discusses using multiple encryption 13 schemes or methods. 14 Q. You don't dispute that Forsberg discloses 15 using multiple public encryption keys, do you? 16 A. Togawa discusses using the public key in their 17 disclosure, which you could assume it could be 18 any one of the number of public keys. 19 Q. Using multiple encryption schemes in a 20 wireless communication wasn't invented at the 21 time of the '817 patent, was it? 22 A. There were, based on the 3GPP standards for 23 example, there were options for different 24 encryption schemes to be utilized. 25 Q. Using multiple public keys in a wireless
Page 91	Page 93
1 declared essential to the 5G standard? 2 A. Declared essential is a term that would 3 encompass the patents being found as essential 4 by a jury, for example, or an ITC case. 5 But I don't know the exact number that 6 Ericsson has that have been declared 7 essential. 8 Q. You, yourself, again without getting into any 9 confidential information, have opined that 10 there are more than one 5G essential patents, 11 correct? 12 A. Correct. 13 Q. Is every 5G essential patent non-obvious? 14 MR. MICHELI: Objection, calls for 15 speculation. 16 A. It would depend upon the context of the 17 patent. I'd have to look at it to see -- to 18 determine if that's the case or not for a 19 given patent. 20 BY MR. RHINE: 21 Q. It would depend on the patent itself, right? 22 A. Well the disclosures in the patent and 23 obviously -- again, going through a case like 24 this, or a case to see if it's stress tested 25 to see if it's obvious or not, and that would	1 communication system wasn't novel at the time 2 of the '817 patent, was it? 3 A. Use of public keys have been around for a long 4 time, certainly multiple public keys have been 5 around for a while. 6 Q. Choosing to use multiple public keys wasn't 7 some big invention, right? 8 A. So again, multiple public keys have been 9 known -- the use of mobile public keys -- 10 multiple public keys was known and included in 11 wireless systems. 12 - - - - 13 (Court reporter clarification.) 14 - - - - 15 BY MR. RHINE: 16 Q. The '817 patent doesn't purport any -- excuse 17 me -- surprising results from using multiple 18 encryption schemes, does it? 19 A. Well, it -- in terms of being able to solve 20 the problem that had been around for decades, 21 it certainly provided -- in my evaluation and 22 from the perspective of a person of ordinary 23 skill in the art working in the field -- 24 that -- that inventive solution, given that it 25 solved that long felt problem -- the problem

24 (Pages 90 to 93)

Page 94 1 that was sought after for a long time -- was 2 surprising. 3 It was something that came out of an 4 unexpected -- it was an unexpected approach to 5 solving that problem for a new architecture. 6 Q. Nair solves the problem of encrypting an IMSI 7 in a 5G network, doesn't it? 8 A. It addresses the use of encrypting IMSI in a 9 specific way in a 5G network. 10 Q. And it works, right, their system would 11 encrypt the IMSI in a 5G network? 12 A. Yes, it would. 13 Q. Why is the use of multiple encryption schemes 14 necessary to solve the problem of encrypting 15 an IMSI? 16 A. Because it -- Nair's system is completely 17 inflexible. 18 In terms of a modern flexible 19 communication system, they had one solution, 20 do it fast and quick, which was great, but it 21 was very limiting. The approach taken with 22 '817 is very different which provides 23 flexibility but provide -- 24 ---- 25 (Knocking on door.)	Page 96 1 and choose your encryption scheme based on the 2 needs of the user as well as the network 3 operator. 4 Q. Does the '817 patent identify a long felt need 5 of needing to change the encryption scheme? 6 A. Yes. 7 Q. Where? 8 A. It's in the entirety of the document, it's 9 what it's disclosed for. It's -- a person of 10 ordinary skill in the art would understand 11 that. 12 Q. It discloses the ability to change an 13 encryption scheme, correct? 14 A. Yes. 15 Q. Does it describe that as a long felt need or 16 a? 17 A. It does not use those words but it's in the 18 context of what we've known for decades of why 19 the system was vulnerable. 20 Q. Do you cite to any evidence that the ability 21 to change an encryption scheme is a long felt 22 need in wireless systems? 23 A. Well, I certainly rely on my experience and 24 working in communications and security areas 25 specifically for DOD entities and other
Page 95 1 ---- 2 MR. RHINE: Go off the record. 3 ---- 4 (Pause in the record.) 5 ---- 6 MR. RHINE: Back on the record. And 7 you can -- 8 THE WITNESS: I'll finish. 9 BY MR. RHINE: 10 Q. You finish, please. 11 A. So it provides for change and growth and 12 evolution is future networks, which again 13 is -- that is -- was a novel approach compared 14 to what was taken before. 15 Q. Well, it sounds like using multiple encryption 16 schemes allows for greater flexibility, but it 17 doesn't -- it isn't required to achieve 18 encrypting an IMSI on a 5G network, correct? 19 A. So you can choose to use a single encryption 20 scheme, correct. 21 Q. Why do you think using multiple encryption 22 schemes solves a long felt need? 23 A. Because it's not just -- and -- it's not just 24 the use of an encryption scheme, it's the use 25 of being able to change your encryption scheme	Page 97 1 elements, that, yeah, that was a need that was 2 out there. 3 Q. Has -- Togawa discloses a method of 4 identifying multiple encryption schemes, 5 doesn't it? 6 A. Togawa is oriented to changing the encryption 7 in a data communications and multimedia voice 8 communications in a legacy system, and you can 9 change the encryption scheme based on the 10 disclosures in Togawa within their -- their 11 architecture. 12 Q. Is it your opinion that Togawa's solution is 13 too basic to be considered in a 5G network? 14 A. No, it's my opinion that it's incompatible 15 with an authentication procedure in a 5G 16 network. 17 Q. Why? 18 A. Because that's not how the authentication 19 procedure would work. 20 Q. I mean, why does that mean, it's incompatible? 21 A. The disclosures in Togawa are specific and 22 they -- they're incompatible with an 23 authentication procedure. 24 Q. I understand that they aren't used in an 25 authentication situation, but why are they

25 (Pages 94 to 97)

Page 98	Page 100
1 incompatible? 2 A. Because it's -- you're not transmitting a 3 stream of data and changing your encryption 4 scheme on the fly. It's a specific set of 5 procedures that are structured in the 3GPP 6 protocols, again, over decades and developed, 7 and that -- that technique on Togawa is just 8 completely incompatible with how you would go 9 through an authentication procedure in a -- 10 with a cellular system. 11 Q. On a scale of 1 to 10, can you rank how 12 inventive it would be to identify an 13 encryption scheme using a mid-field? 14 MR. MICHELI: Objection. 15 A. I'm not sure -- I would need context. It 16 would need basically specifics and metrics. 17 I'm not sure what you're getting to. 18 BY MR. RHINE: 19 Q. I'm getting to -- this invention seems a 20 little weak, you need to know which encryption 21 scheme to use so you tell the decryption 22 server which encryption to use, what is 23 inventive about that? 24 A. Well, I've already answered that several 25 times, and I would just go back to my previous	1 it to be combined with Forsberg? 2 A. Nair's system is completely incompatible with 3 Forsberg because Nair's system is directed to 4 using a single public/private key pair. I 5 don't know how else to describe that. 6 Q. In Paragraph 108 of your declaration, in the 7 middle of the paragraph, you say, Conversely 8 Nair only including the use of a single SLF. 9 A. I see that. 10 Q. Is that the basis of your opinion that Nair 11 only describes a single public/private key 12 pair? 13 A. I'm just pointing out that Nair has two 14 configurations, one includes a single SLF is 15 what I'm pointing out in this paragraph. 16 MR. RHINE: Okay. Can we go off the 17 record? 18 - - - - 19 (Pause in the record.) 20 - - - - 21 MR. RHINE: Good afternoon, 22 Dr. Mahon. 23 THE WITNESS: Good afternoon. 24 BY MR. RHINE: 25 Q. I would like to ask you some questions about
Page 99	Page 101
1 answers. Someone who's worked in the field 2 for decades, looking at the solution, knowing 3 the problem's coming up at this point and the 4 solution that is provided is elegant and it's 5 -- it integrates well and it provides for 6 future flexibility. 7 Q. Can we turn to Paragraph 89 of your 8 declaration? 9 A. Okay. 10 Q. You dispute that a person of ordinary skill in 11 the art would be motivated to combine Nair and 12 Forsberg, because Nair does not teach managing 13 multiple public and private key pairs, 14 correct? 15 A. That is correct. 16 Q. Forsberg does teach managing multiple public 17 and private key pairs, correct? 18 A. Forsberg discloses the use of public keys, it 19 doesn't specifically talk about how to manage 20 multiple public/private key pairs. But within 21 its disclosure it's certainly flexible enough 22 to -- to implement multiple public -- public 23 keys, and therefore, private key pairs. 24 Q. In your opinion, does Nair need to teach the 25 use of multiple public key pairs in order for	1 the Togawa reference, that's Exhibit 2006, and 2 if you would go to Figure 9. 3 Now Figure 9 discloses two communication 4 paths, user data -- user data communication 5 path 70 and voice signal communication path 6 80, correct? 7 A. Correct. 8 Q. In the context of Togawa, user data is not the 9 same thing as a voice signal, correct? 10 A. Togawa's description of Figure 9 says that it 11 depicts the functional configuration of the 12 communication system, according to the second 13 embodiment. And as shown in the Figure 9, in 14 the communication system, the data 15 transmitting apparatus 50 and the data 16 receiving apparatus 60 are connected through a 17 user communication path and a voice 18 communication path. 19 So it's distinguishing user data from a 20 voice signal communication path, but it's 21 describing the transmitter and receiver both 22 as data receiving and data transmitting. It's 23 showing a separate path for the voice signal. 24 So this configuration is showing handling 25 two different streams, one associated with

26 (Pages 98 to 101)

Page 102	Page 104
1 voice signal and one it terms is user data, is 2 what Togawa seems to be disclosing here. 3 Q. So it's fair to say that Togawa is 4 distinguishing between user data and voice 5 signal information, correct? 6 A. That's reasonable to say, yes. 7 Q. It's the user data that is encrypted in 8 Togawa, correct? 9 A. Well, it's encrypting both here, it's 10 encrypting -- it's showing an encryption 11 processor that's taking the input of the voice 12 as well as another input device, based on this 13 diagram. 14 Q. The voice signal carries the encryption 15 specification information, correct? 16 A. That is correct. 17 Q. That encryption specification information is 18 used to encrypt the user data, correct? 19 A. Correct. 20 Q. But the voice signal itself is not encrypted? 21 A. They are describing what they call a voice 22 signal as not being encryption -- encrypted 23 here. 24 Q. Togawa doesn't relate to the encryption of 25 voice signals, right?	1 being applicable to non-voice signals, for 2 example, versus voice signals. It seems to 3 encompass both. 4 Q. If we go to Column 14 starting at Line 16, 5 Togawa discloses a transmitting apparatus that 6 is an apparatus that encrypts user data and 7 transmits the encrypted data. 8 Do you see that? 9 A. Yes. 10 Q. Togawa is directed towards encrypting user 11 data, correct? 12 A. It's -- it's directed towards encrypting user 13 data, which again, I don't see it specifically 14 excluding voice data from that. 15 MR. RHINE: No further questions. 16 Thank you, Dr. Mahon. 17 MR. MICHELI: Let's go off the 18 record. 19 ---- 20 (Pause in the record.) 21 ---- 22 MR. MICHELI: Back on. 23 Dr. Mahon, I have a few follow up 24 questions for. 25 ----
Page 103	Page 105
1 A. Well, Togawa is directed to a legacy system. 2 They are disclosing that they are using what 3 would be termed a call setup, or a call 4 structure within the legacy system for 5 carrying, essentially, overhead information 6 associated with the encryption, and that 7 they're using that for decrypting the data, or 8 transmitting the encryption keys over the 9 connection. 10 Q. But Togawa is directed towards encrypting user 11 data, correct? 12 A. So specifically in Column 1, Togawa says, with 13 respect to the background of the invention, 14 that an integrated communication service that 15 carries out data communications of user data, 16 as well as bidirectional communications of 17 multiple media information, such as voice 18 data, for voice call, and image data for a 19 video telephone, has been provided. When data 20 to be transmitted must be protected from 21 interception by a third party, the data is 22 encrypted. 23 Then it goes on in the invention section 24 to discuss further details, and I don't see 25 them differentiating between the data term	1 CROSS EXAMINATION 2 ---- 3 BY MR. MICHELI: 4 Q. You recall that counsel asked you about, 5 first, could you please turn to Exhibit 1004, 6 which is Nair? 7 A. Yes. 8 Q. Do you recall that counsel asked you about 9 Nair's Paragraph 42 earlier, right? 10 A. Yes, I do. 11 Q. And is it your understanding that Nair claims 12 priority to a provisional application? 13 A. Yes, it does. 14 Q. Did you review the Nair provisional patent 15 application? 16 A. Yes, I did. 17 Q. And from your review, was Paragraph 42 of the 18 Nair application that we're looking at here 19 reflected in that provisional application? 20 A. Based on my review, no, it was not, and there 21 were additional elements that were not 22 supported in that provisional application, 23 based on my review. 24 Q. What additional elements were not supported in 25 that provisional application based to your

27 (Pages 102 to 105)

Page 106	Page 108
1 review? 2 MR. RHINE: Objection, scope. 3 A. The authentication server and the deconcealing 4 server were another -- other examples that I 5 did not see supported in the provisional. 6 BY MR. MICHELI: 7 Q. Earlier counsel asked you why it matters if 8 the Nair trial and error approach worked with 9 multiple encryption schemes. 10 Do you recall that? 11 A. Yes, I do. 12 Q. Is Nair's preferred privacy indicator 13 compatible with multiple encryption schemes? 14 A. No. 15 Q. So is the trial and error approach 16 incompatible with multiple encryption schemes? 17 A. Is it compatible? 18 Q. (Indicating.) 19 A. No. 20 Q. Is there anything disclosed in there that is 21 compatible with multiple encryption schemes? 22 A. No. 23 Q. What is the 3GPP? 24 ---- 25 (Court reporter clarification.)	1 communication system itself. 2 So yes, it would be considered laudable. 3 MR. MICHELI: Thank you. No more 4 questions. 5 ---- 6 REDIRECT EXAMINATION 7 ---- 8 MR. RHINE: Dr. Mahon, I have a few 9 questions for you. 10 THE WITNESS: Yes. 11 MR. RHINE: Can I introduce what is 12 previously marked as Exhibit No. 1008. 13 ---- 14 (Exhibit No. 1008 was previously marked for 15 identification.) 16 ---- 17 BY MR. RHINE: 18 Q. Dr. Mahon, is this the Nair provisional you 19 were just referring to? 20 A. Yes, it is. 21 Q. Do you mind turning to Figure 6, which is on 22 Page 19? 23 A. Figure 6, Page 19, yes. 24 Q. Figure 6 in the provisional, is substantially 25 similar to Figure 6 in the published Nair,
Page 107	Page 109
1 ---- 2 MR. MICHELI: 3GPP. 3 A. Third Generation Partnership Project. 4 BY MR. MICHELI: 5 Q. It's an organization, right? 6 A. It is an organization made up of, basically, 7 engineers and corporations across the world. 8 Q. Is it considered an accomplishment to have -- 9 for an engineer to have their technology 10 incorporated into a standard maintained by 11 3GPP? 12 A. Well how the standard bodies work, they are 13 trying to solve problems and come up with 14 solutions for the next generation standards. 15 And they submit -- engineers submit proposals 16 of their technical solutions, which are 17 considered by the boards and standards bodies. 18 And basically there is a debate and evaluation 19 and analysis that goes on. 20 So essentially when an idea is 21 incorporated or approved by a standards body, 22 and incorporated into the standards, it's 23 chosen for many factors. One being the 24 technical -- technical value, meaning what 25 does it brick to the table for the	1 Exhibit No. 1004, right? 2 A. Yes. 3 Q. Figure 6 discloses an AMF in the provisional? 4 A. It does show an AMF pictured in that figure. 5 Q. And it does show an AUSF? 6 A. It does show that. 7 Q. You don't dispute that AUSF is an 8 authentication server, correct? 9 A. The only thing I'm -- in terms of support 10 within the provisional, is that the 11 provisional just gives a brief description of 12 what these elements, it doesn't talk about 13 what aspects of the messages they are working 14 on. It shows these elements and provides like 15 a one or two word description of them. 16 But an AUSF would be understood by a 17 person of ordinary skill in the arts to be an 18 authentication server. 19 Q. An AUSF would be understood by a person with 20 skill in the art to be a deconcealing server, 21 correct? 22 A. Well, it shows that the SLF is performing a 23 decryption, and as we discussed before, a 24 POSITA would understand that a deconcealing 25 server does perform that same function.

28 (Pages 106 to 109)

Page 110 1 Q. Is it your opinion that Nair's provisional 2 doesn't describe the null encryption scheme? 3 A. Null encryption scheme is not contained in the 4 provisional. 5 Q. But Nair teaches to not encrypt the IMSI, 6 right? 7 A. The -- 8 Q. Sorry, let me strike that. 9 Nair discloses a situation where the IMSI 10 is not encrypted, correct? 11 A. In the Nair patent, it does disclose that 12 there is a situation where the IMSI may not be 13 encrypted. 14 Q. And as we discussed a couple times today, a 15 null encryption scheme is just not encrypting, 16 correct? 17 A. Null encryption would be understood by a 18 POSITA as to be not encrypting the 19 information. 20 Q. Why do you think that the Nair provisional 21 doesn't describe the null encryption scheme? 22 A. Well, the provisional doesn't use that term. 23 In terms of what it means or what it would 24 mean by a null encryption, that's what I'm 25 pointing to.	Page 112 1 Q. And so when the flag is not flagged the IMSI 2 is not encrypted? 3 A. It specifically said, If not set the network 4 will presume that the IMSI is unencrypted. 5 Q. And when it is provided unencrypted, that is 6 null encrypted, correct? 7 A. When it is unencrypted, and it doesn't use the 8 term or phrase "null encryption," but 9 effectively, it's the same to a POSITA. 10 Q. Can we go please to your declaration, the 11 materials reviewed section, Paragraph 20? 12 A. Okay, I'm there. 13 Q. You didn't rely on any 3GPP -- strike that. 14 MR. RHINE: No further questions. 15 MR. MICHELI: No further questions. 16 ---- 17 (Thereupon, the deposition was concluded at 1:00 18 P.m.) 19 ---- 20 21 22 23 24 25
Page 111 1 Q. You are just saying that it doesn't use the 2 word "null encryption scheme" -- or the words 3 "null encryption scheme"? 4 A. Null encryption is not used at all in the 5 provisional application. 6 Q. But not encrypting the IMSI is used in the 7 provisional application, correct? 8 ---- 9 (Witness reviewing document.) 10 ---- 11 BY MR. RHINE: 12 Q. Please keep reviewing if you want, but Page 6 13 of the provisional, Page 26 of the document, 14 Lines 17 through 18 might be helpful to look 15 at. 16 A. Page 6 you said? 17 Q. 6 of the provisional, Page 26 of the exhibit. 18 A. Thank you. 19 Q. So here, the Nair provisional discloses the 20 use of identity privacy flag or privacy 21 indicator, do you see that? 22 A. I do. 23 Q. That indicates that the IMSI is provided 24 encrypted? 25 A. Correct.	Page 113 1 COMMONWEALTH OF PENNSYLVANIA) CERTIFICATE 2) 3 COUNTY OF ALLEGHENY) SS: 4 I, Anna Cillo, a Court Reporter and Notary 5 Public in and for the Commonwealth of Pennsylvania, 6 do hereby certify that the witness, DR. MARK MAHON, 7 was by me first duly sworn to testify to the truth; 8 that the foregoing deposition was taken at the time 9 and place stated herein; and that the said 10 deposition was recorded stenographically by me and 11 then reduced to printing under my direction, and 12 constitutes a true record of the testimony given by 13 said witness. 14 I further certify that I am not a relative or 15 employee of any of the parties, or a relative or 16 employee of either counsel, and that I am in no way 17 interested directly or indirectly in this action. 18 IN WITNESS WHEREOF, I have hereunto set my 19 hand and affixed my seal of office this __ day of 20 _____, 2025. 21 22 _____ 23 Notary Public 24 25

29 (Pages 110 to 113)

DEPOSITION ERRATA SHEET		
PAGE	LINE	CHANGE REASON
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24	DR. MARK MAHON	DATE
25		

A ability 14:13,21 96:12,20 able 10:2 13:24 19:24 22:17 26:12 28:22 29:1 46:25 53:16 63:16 67:5 68:13 93:19 95:25 access 23:11,13 accommodate 14:19 accomplishment 107:8 accuracy 84:19 accurate 6:14 10:17 54:5 achieve 24:5 95:17 acquire 7:14 acronym 10:2 14:3 15:14 70:11 72:16 72:25 action 113:16 adding 27:20 additional 45:19 78:3 79:12 105:21 105:24 address 37:7 59:14 82:25 85:15,15 addressed 48:15 81:9 addresses 47:24 66:22 67:1 83:5 83:10 94:8 addressing 83:7 adopted 90:15 92:6 adoption 90:2,11 90:13 92:2 affixed 113:18 afternoon 100:21 100:23 ago 7:15 agree 15:24 28:25 36:12 68:19 73:19 80:24 82:5 89:14 agreed 55:15 agreeing 49:7 agreement 55:16	ahead 54:23 55:16 air 13:15 37:2 81:12 al 4:8,10 algorithms 9:15 alleged 13:1 20:4 ALLEGHENY 113:2 allocated 71:9 allow 14:17 allowed 18:22 allows 18:16 20:25 52:24 68:22 69:1 95:16 alternative 35:9 60:5 61:5 62:18 ambiguity 63:8 AMF 39:21 42:1,2 87:2,9,18 88:1,11 109:3,4 AMF's 88:3 analysis 107:19 anchored 18:5 Anna 1:23 2:2 113:3 answer 6:2,3,7 60:1 77:9 answered 61:8 64:5 78:16 98:24 answering 6:6 answers 99:1 anybody 11:21 apparatus 52:18 101:15,16 104:5,6 APPEAL 1:3 APPEARANCES 2:7 appearing 6:16 appears 7:5 applicable 104:1 application 4:7,10 4:12 105:12,15,18 105:19,22,25 111:5,7 applied 15:14 apply 77:11 applying 23:10	approach 54:21 94:4,21 95:13 106:8,15 appropriately 52:20 88:13 approved 107:21 approximately 12:9 architecture 13:5 19:2,6,8,20 65:6 66:15 77:5,7 94:5 97:11 area 7:16 9:2,10 65:2 areas 8:24 50:4 81:5,8 96:24 argument 76:6 arrives 42:8 art 11:8 15:25 16:4 16:8 17:10 18:25 21:15,18,19,23 22:3 23:7 24:5,8 27:17,25 43:6,11 44:19 62:14 65:1 65:13 76:8 84:2 85:6 89:1 93:23 96:10 99:11 109:20 arts 109:17 aside 12:12 asked 8:10 60:3 61:7 64:4 78:15 105:4,8 106:7 asking 6:7 8:18 10:19 aspect 14:11 60:16 60:22 66:7,9,10 72:18 aspects 8:2 9:1 60:21 65:8 109:13 asserting 49:20 assistance 74:18 associated 9:1,6 16:16 21:24 24:1 31:1 34:8 39:10 48:3 68:25 69:5 69:11 70:1 71:22	86:20 101:25 103:6 assume 5:25 54:20 87:8 92:17 attach 59:15,18 attached 45:14 55:21 attacks 14:1 attempt 54:6 attempted 13:24 attempting 54:12 attempts 18:9,19 attend 8:5,15 attention 47:16 65:22 attorneys 11:20 12:12 AUSF 39:25 40:2 40:18 41:14,16,17 41:20,23 42:2,5,8 42:12,14 87:14,16 87:19,21,23,24 88:16 109:5,7,16 109:19 authenticate 67:6 71:7 authenticating 50:11 79:8 authentication 18:12 19:9,11,12 19:23 22:24 37:12 37:14 38:6 40:3 41:8,11 42:1 50:9 57:10 58:23 59:2 59:15 60:10 61:11 65:3,10 66:18,20 74:24 78:20 79:4 79:20,21 87:19,22 88:16,19 89:16 97:15,18,23,25 98:9 106:3 109:8 109:18 automatically 79:23 available 84:6 Avenue 1:20 2:10 aware 84:5	a.m 1:15 2:5 B B 56:3,8 back 21:5 22:18 36:4 51:11 52:4 53:2 57:18 59:2 60:4 66:12 69:14 74:9,15 75:3,9 78:25 80:4 95:6 98:25 104:22 background 103:13 based 19:24 20:2 29:13,15 32:20 33:3 41:2,6 45:5 48:17 49:8 59:1 61:21 83:23 88:6 88:14,22,23 92:7 92:22 96:1 97:9 102:12 105:20,23 105:25 basic 97:13 basically 26:20 57:20 86:18 98:16 107:6,18 basis 100:10 began 7:15,18 beginning 23:18 49:11 beneficial 24:11 benefit 26:9 70:4 best 77:8 better 55:1 beyond 25:8 bidirectional 103:16 big 93:7 Bims 11:7,11 64:18 64:21 bit 5:21 29:7 57:16 59:11 86:7 bits 17:22 23:24 blind 53:12,24 57:20 Blinded 53:14 BOARD 1:3
--	--	--	---	--

boards 107:17	26:2 41:3 61:3	class 82:2	compatible 43:17	contains 73:3
bodies 107:12,17	69:25 70:12 72:11	classes 82:2	62:20 66:15	contemplates 35:19
body 107:21	75:6 84:6 87:6	clear 13:8 30:4	106:13,17,21	68:8
Boolean 55:25	93:4,21 96:23	36:20	competing 92:4	content 73:17
60:16 62:3	99:21	clearance 8:13	complete 6:13	contents 15:18
bottom 28:20 43:20	CERTIFICATE	code 70:19,20	completely 94:16	19:25 31:2
Boulevard 2:4	3:6 113:1	coined 14:3	98:8 100:2	context 11:18
bouncing 39:11	certify 113:5,13	College 2:4	comprises 38:20	15:20 16:6,9,20
break 6:9,11 26:14	cetera 33:13,18	column 35:1 43:21	71:13	19:18 21:3,25
26:24 45:21,24,25	35:6	43:21 47:16,23	computation 84:16	24:24 25:9,23,25
47:3 85:25	change 49:12 73:9	48:11,16 51:12,18	computational	28:21 34:21 40:15
brick 107:25	95:11,25 96:5,12	52:4,6,13,22	26:15 54:24	40:24 42:10 46:13
brief 11:13,17	96:21 97:9 114:2	103:12 104:4	conceal 37:10	46:19 49:5 50:16
109:11	changed 20:11	combine 64:14,16	83:11	56:5,6 57:11
bring 47:16 65:22	changing 20:8	64:22 65:13 99:11	concealing 82:25	58:17,18 59:23
broad 53:14,25	48:16 97:6 98:3	combined 56:17	83:5,10,15,22	60:2 62:11 66:22
broader 59:23,24	characteristic 27:1	100:1	84:2	73:24 75:23 76:5
broadly 90:5	charm 27:13	come 18:13 59:11	concept 25:13,19	76:11,16,17 77:21
	choice 84:15,22	107:13	concerned 78:5	78:8,13,21 86:16
C	90:15	coming 99:3	concluded 112:17	86:24 87:7 90:17
call 102:21 103:3,3	choose 56:8 62:23	commencing 2:5	Conference 2:4	91:16 96:18 98:15
103:18	63:23 95:19 96:1	commercial 8:18	confidential 90:24	101:8
called 2:1 13:7	chooses 58:18	8:19	91:9	contexts 59:17
37:24 53:12	Choosing 93:6	commonality 29:5	configuration	continue 90:5
calls 19:11 23:16	chose 55:17	Commonwealth	101:11,24	contributions 90:3
23:21 60:15 66:24	chosen 58:15	2:3 113:1,4	configurations	control 13:12 23:13
91:14	107:23	communicated	86:19 100:14	25:17 26:1 49:10
capability 29:19	Cillo 1:23 2:2 113:3	16:13 51:2,8	conjunction 22:7	65:4
captured 36:19	circuitry 38:21,21	communicating	connect 23:15	Conversely 100:7
carriers 90:6	38:25 39:1,4	37:1 58:6	connected 101:16	corner 61:4 80:20
carries 102:14	cite 90:13 96:20	communication 7:7	connection 103:9	corners 16:25
103:15	cited 11:8,24 30:2	7:18,25 8:2 9:17	consider 7:9,12	corporations 107:7
carrying 42:2	citing 27:18	20:8 36:9 47:18	23:6 76:17 84:4	correct 6:17,18 7:2
103:5	Civil 2:2	47:19,19,25 63:20	considered 15:22	10:15,20 15:9
case 1:7 9:9,19 10:4	claim 16:17 17:9	66:6,23 67:3,3	85:1 97:13 107:8	17:13 21:16,21
25:5 27:24 33:18	40:25 41:5,8,13	92:20 93:1 94:19	107:17 108:2	23:22 24:17,18,20
40:20 61:4 62:8	42:13 46:8,11	101:3,4,5,12,14	consists 70:18	25:15 28:8,9,16
91:4,18,23,24	49:5 77:3 78:5,11	101:17,18,20	constitutes 113:11	28:23,24 29:14,20
cases 9:19	79:14,16,18	103:14 108:1	construct 13:7	30:11,16,25 31:15
caveats 78:23	claims 17:17 42:10	communications	16:11 30:22 45:5	31:19 32:2,5,17
cellular 7:23 9:8,17	68:15 77:1 78:2	7:24 9:9 13:13	contain 25:4 43:24	33:8,11 34:7,10
23:20 25:14 65:25	105:11	14:22 25:15 48:9	72:19 74:13	34:19 35:4,20
66:6,8,24 98:10	clarification 9:22	50:6 53:15 59:12	contained 15:12,12	36:10,20 37:3,13
Center 2:4	21:10 27:6 35:15	65:8,25 66:8	32:10 50:10 87:17	37:25 38:4,12,18
certain 33:21 78:9	37:18 82:19 93:13	96:24 97:7,8	110:3	39:15,21,22 40:24
certainly 10:5	106:25	103:15,16	containing 20:1	41:19,24 42:6
14:25 17:14 19:12	clarity 35:8	compared 95:13	74:3	43:1,2,23 44:2

46:7,10,24 47:20 48:1,14 50:20 51:2,22 52:2,3,10 52:20,25 53:9,10 53:13 55:13 56:15 58:20 60:7 61:1,6 62:16 63:18 65:25 66:14,24 67:13,19 67:20 68:20,25 69:20,22 70:21,22 71:9 72:4,7 74:4,7 74:8,12,20 75:12 75:16 76:10 77:2 77:25 79:2,5 80:12,15 81:1,6 81:25 83:1,6,17 83:23 84:4,9 85:5 85:24 86:14 87:20 87:23,24,25 88:8 88:9,17,18,21 89:6,7,9 90:12,22 90:23 91:11,12 92:11 95:18,20 96:13 99:14,15,17 101:6,7,9 102:5,8 102:15,16,18,19 103:11 104:11 109:8,21 110:10 110:16 111:7,25 112:6 correctly 58:15 correspond 33:8 counsel 1:18 4:15 11:1 12:4,7 105:4 105:8 106:7 113:15 counting 34:12 country 70:19 COUNTY 113:2 couple 73:7 110:14 coupling 69:2 course 35:9 court 2:2,15 3:6 6:2 9:22 21:10 27:6 35:15 37:18 82:19 93:13 106:25 113:3	Crescent 2:15 CROSS 3:4 105:1 cryptography 84:15 Curriculum 4:4 curve 26:6,9,12,17 27:15 84:15 CV 7:2 D Dallas 2:16 data 23:14,22,25 24:1,6,10 26:1 29:5 47:18,21,25 48:3,3,5,6 50:6,8 50:20 51:22 52:1 52:18,24 65:6,10 67:2 97:7 98:3 101:4,4,8,14,15 101:19,22,22 102:1,4,7,18 103:7,11,15,15,18 103:18,19,21,25 104:6,7,11,13,14 date 1:14 7:4 10:3 85:6 114:24 day 113:18 days 12:13 dealing 8:1 35:25 debate 107:18 decades 7:22 9:6 13:19 18:7 70:24 71:2 83:19 92:5 93:20 96:18 98:6 99:2 decided 20:12 49:9 declaration 4:5 10:14,17,24 11:5 11:11,21,25 28:18 30:8 45:10,11 53:2 89:22 99:8 100:6 112:10 declared 91:1,2,6 decode 62:6 decoded 57:15,16 decoding 53:13,24 63:18	deconceal 75:17 deconcealing 13:17 40:9,13,16,19,23 41:6,9,12,14 46:20 74:25 75:1 75:21 76:2,4,5,10 76:18,20,25 77:2 77:12,13,16 78:7 78:13 106:3 109:20,24 deconcealment 75:24 deconceals 75:15 decreased 81:5 decrypt 38:15 41:10 43:15 54:6 54:12,17 55:20 56:7,9 58:22 60:19 68:24 69:9 69:20 75:7,17 decrypted 58:9 decrypting 74:19 78:1 103:7 decryption 19:14 19:17,17 21:4,21 22:19 33:1 40:12 40:14,20,21 41:2 41:4,18 43:7,13 43:17 45:18 46:6 46:22 47:1 51:10 57:3 58:9,14 59:10 68:13 69:13 75:4,10,24 76:3 76:10,16 77:17 78:4 79:1 98:21 109:23 decrypts 40:11 75:11 defines 29:17 definitely 66:4 depend 23:3 91:16 91:21 depends 88:20 90:17 depicted 41:21 42:8 depicts 101:11	deployed 90:5 deposition 1:12,14 1:16 2:1 5:22 11:12,19 12:3,5,8 12:20 112:17 113:7,9 114:1 describe 77:21 96:15 100:5 110:2 110:21 described 83:21 describes 81:14,22 81:22 100:11 describing 101:21 102:21 description 35:8 71:20 101:10 109:11,15 design 20:15 90:15 designed 30:5 desirable 26:25 details 103:24 detect 53:11,20,23 54:2 determine 49:16 69:1 89:15 91:18 determined 41:15 57:17 determines 41:9 determining 59:21 developed 8:16,21 98:6 developers 84:21 development 8:3 device 14:18 32:25 32:25 39:3,9 46:5 58:18 59:19 79:5 102:12 devices 21:2 84:16 84:23 diagram 42:9 102:13 difference 48:25 49:20 different 20:22 21:1 22:2 23:1 50:4 55:11,17 65:7 69:5 70:6	76:13 89:5 92:23 94:22 101:25 differentiating 103:25 direct 86:10 directed 36:16,21 37:14 38:5 62:24 100:3 103:1,10 104:10,12 directing 36:2 direction 113:10 directly 42:12 113:16 disagree 29:21 disclose 17:22 28:13 32:10 75:1 75:2 110:11 disclosed 15:10 16:12 22:13,20 39:18 40:10 41:22 48:18,23 49:14 50:14,14,16,23 64:19 68:3 72:15 72:21 73:1,1,15 73:18 75:5 76:12 77:6 86:19 96:9 106:20 discloses 16:5 17:20 19:23 32:11 37:24 38:11,18,25 39:14,17,20 43:22 48:12,16,21 49:3 54:15 55:8 56:6 56:14,16 70:9,12 70:13,15 71:12,16 71:19 72:3,22 73:10,19,21 74:3 74:13,15,18,22 78:9 81:11 92:14 96:12 97:3 99:18 101:3 104:5 109:3 110:9 111:19 disclosing 19:19 64:19 102:2 103:2 disclosure 13:4 16:24 17:1 19:4 29:24 30:3 34:8
---	--	---	---	---

34:20 35:21,24 38:9,13 73:8 75:23 92:17 99:21 disclosures 40:25 77:4,14 91:22 97:10,21 discuss 12:2 83:24 103:24 discussed 28:10 49:4 63:24 70:18 109:23 110:14 discusses 82:9,24 83:13 87:7 92:12 92:16 discussing 27:24 55:9 57:11 60:6 61:25 64:13 68:18 83:2 86:13,25 discussion 30:3 59:24 dispute 48:19 64:23,25 65:12 67:8 70:9,13 71:12 72:20 74:22 76:1 78:6,24 83:9 84:19,21 85:12 92:10,14 99:10 109:7 disputing 38:24 39:14,16 40:2,8 40:22 72:22 78:12 78:17,19 distinction 73:15 87:4 distinguishing 101:19 102:4 district 36:5 doc 33:20 document 32:13 84:7 85:6 96:8 111:9,13 documents 11:6,9 11:14,23 27:24 84:5 DOD 8:10 96:25 doing 7:22 8:14,23 9:1,10 40:18 54:7	56:11 60:25 63:25 75:9 door 94:25 Dr 1:12 2:1 3:3 4:4 4:5 5:9 7:2 10:14 11:7,11 31:11 34:5 64:18,21 100:22 104:16,23 108:8,18 113:5 114:24 draft 10:23,25 draw 73:14 due 8:12 57:15 72:17,17 90:1 duly 5:10 113:6 D.C 1:21 2:11 E E 31:18 earlier 68:18 105:9 106:7 ECIES 27:20 28:1 28:15 32:16,19 33:2 68:11 83:3 83:23,24 84:22 85:3,8 effectively 44:3 112:9 efficiency 55:7 62:25 efficient 24:5,10 38:5 52:24 60:9 61:2,11,18 63:20 efficiently 21:6 26:20 efforts 37:6 either 59:3 62:23 87:10 113:15 electric 84:14 elegant 99:4 element 39:25 41:13 42:13 72:21 76:15 79:16 87:16 elements 13:8 16:14,17 17:9 18:12 19:5,8 35:6 35:10,12,13 42:15	49:5 51:9 65:7 67:24 68:3 77:3,6 78:5 79:18 87:5 97:1 105:21,24 109:12,14 eliminate 60:1 elliptic 26:6,9,11 26:17 27:15 ELLIS 1:20 2:10 embodiment 35:7,9 101:13 employee 113:14 113:15 enable 20:21 enclave 89:11 encode 20:3 encoding 53:14 encompass 91:3 104:3 encompassed 18:2 68:16 encrypt 14:13 15:8 16:2 24:22 43:9 50:20 51:1,7 72:10 85:4,8 94:11 102:18 110:5 encrypted 13:9 14:23 15:24 26:3 26:4 31:2 38:15 39:21 40:11,14,17 41:10,18,23 42:3 42:5 43:12,13 44:12 45:1,8 48:21 54:9,17,19 54:20 56:1 59:6 62:10 67:7,18 68:24 69:9 72:2,3 72:4,6,12,13,14 73:16 74:4,7,11 74:11,14,16,23 75:3,11,15,25 82:6 102:7,20,22 103:22 104:7 110:10,13 111:24 112:2,6 encrypting 15:18	25:14,19 36:22 37:15 42:7 44:2,4 47:18,21,25 67:2 67:11 83:3,7,13 85:13,17,22,23 94:6,8,14 95:18 102:9,10 103:10 104:10,12 110:15 110:18 111:6 encryption 14:16 14:19 16:3,5,19 16:22 17:3,6,7,11 17:12,15,18,24 18:1,21 19:16,22 20:2,5,10 21:21 21:25 22:7 24:14 24:16,17,19,21 25:16,17 26:7,10 26:13,13,18,21,22 26:24,25 27:16 28:2,6,8,11 29:10 29:12,18 30:5,15 30:19,24 31:14,17 31:22,23 32:1,24 33:4,8,10,14,16 33:17,19 34:5 37:10 43:8,14,18 43:22,25 44:1,6 44:16,21 45:2,5 45:13 46:23 48:7 48:8,13,13,16,20 48:23,25 49:1,3,9 49:12,17,18,21,21 49:25 50:13,18,19 50:21,22,24,24,25 51:1,5,5,6,7,10,19 51:21,22,24,25 52:1,5,8,9,10,16 52:17,19,23 53:7 53:9,11,20,21,23 54:13 55:5,11,16 55:18,23 56:18,25 57:7,22 58:7,14 58:16,19 59:5,7,9 60:17,18,21 61:22 62:2,5,7,21 63:2,7 64:3,12,20 68:1,4	70:6 79:13 81:15 81:23 82:3 83:3,8 83:12,14,23 85:2 92:11,12,15,19,24 93:18 94:13 95:15 95:19,21,24,25 96:1,5,13,21 97:4 97:6,9 98:3,13,20 98:22 102:10,14 102:17,22,24 103:6,8 106:9,13 106:16,21 110:2,3 110:15,17,21,24 111:2,3,4 112:8 encryption's 54:3 62:4,5 encrypts 104:6 ends 61:23 engineer 107:9 engineers 107:7,15 entire 14:11 16:24 22:14,19 29:15 entirety 80:15,16 80:22,25 96:8 entities 96:25 entity 74:20 equals 44:7 equipment 71:7 Ericsson 1:9 5:7 6:17 12:17 27:20 90:25 91:6 Ericsson's 11:14 12:12 27:23 ERRATA 114:1 error 54:25 55:2,4 58:11,25 59:4,6 60:6,13,24 61:1,4 61:6,17 62:15,19 62:20 63:1,18,21 63:25 64:8,10,18 106:8,15 errors 57:15,16 59:11 Esq 1:19 2:9,14 essential 90:18 91:1,2,3,7,10,13 essentially 103:5
---	--	---	--	--

107:20 et 4:8,10 33:12,18 35:6 evaluation 77:22 93:21 107:18 events 78:10 evidence 90:9 92:2 92:8 96:20 evolution 95:12 exact 10:3 90:20 91:5 exactly 11:3 examination 2:1 3:1 5:13 105:1 108:6 examined 5:11 example 7:24 8:24 15:21 26:3 28:10 28:15 30:13 31:21 33:10 42:4 56:2 57:14 59:17 68:9 68:11 69:15 70:8 72:6,12,14 78:20 91:4 92:23 104:2 examples 29:13 31:23 106:4 exchange 24:6,11 49:13 52:18,25 excluding 104:14 excuse 76:7 93:16 exemplary 31:25 exhibit 4:1 6:20,23 10:8,12 28:18 31:5,7 33:23 34:2 36:5 47:9,11 65:16,18 66:3 80:4,6 82:11,13 86:7 101:1 105:5 108:12,14 109:1 111:17 exhibits 4:15 existed 13:18 18:7 expect 38:20 46:18 46:20 expected 45:14 experience 9:4,6 92:8 96:23	expert 6:16 7:6,9 7:12 expertise 7:14 experts 12:16 explains 35:3 82:5 explanation 61:24 exposing 15:6 exposure 13:21 expressly 29:17,23 80:14,24 extra 55:6 F fact 15:15 46:19 56:17 61:25 factors 107:23 failed 56:24 57:3 58:16 63:6,16 fails 58:10 failure 55:19 fair 102:3 fall 11:2 falls 72:11 far 78:4 fashion 15:3 fashions 57:3 fast 38:5 60:10 61:11 63:19 94:20 faster 84:16 feature 22:12 features 36:8 February 1:14 2:4 Federal 2:2 feel 12:19 felt 93:25 95:22 96:4,15,21 fewer 38:4,12 field 22:21 25:3,7,8 25:10 36:13 64:24 65:24 66:5 67:9 79:12 93:23 99:1 fields 13:10 14:9 23:1 26:3 68:4,6 68:14 fifth 7:20 9:12 figure 26:16 30:10 30:18,21 31:11,14	31:25 33:11,20 35:3,7 39:23 40:5 40:10,23 41:17,21 41:22,25 62:10 67:15 69:15 74:9 79:7,11,22 85:19 85:22 86:10,12,13 87:18 88:12 101:2 101:3,10,13 108:21,23,24,25 109:3,4 figures 68:5,6 85:20 find 24:10 53:18 75:7 fine 46:1 finish 6:5,6 95:8,10 first 7:19 10:1,23 12:23 27:15,19 28:1 59:19 79:19 87:2,24 105:5 113:6 flag 42:23 43:4 44:23 55:25 62:3 63:23,24 111:20 112:1 flagged 112:1 flexibility 14:18 20:6,7,9,14,22 30:1 94:23 95:16 99:6 flexible 94:18 99:21 flexibly 20:25 flow 42:8 fly 98:4 focused 7:23 8:1 13:3 50:5 55:22 65:3 focusing 35:22 follow 59:21 104:23 follows 5:11 footnote 28:20 foregoing 113:7 form 39:21 format 17:18	forming 76:24 Forsberg 4:10 64:15 66:1,2,5,22 67:1,5,8,11,16,18 67:25 68:19 69:7 69:16,18,23 70:9 70:11,13,18 71:8 71:10,12,16,19 72:2,3,22 73:4,10 73:16,19 74:1,3,6 74:9,13,15,18,22 75:1,11,14,23 76:12 77:23 78:20 78:25 79:4,11 92:14 99:12,16,18 100:1,3 Forsberg's 68:22 71:25 78:6,12 forward 5:22 11:9 34:25 88:13 forwarding 74:24 found 91:3 four 9:16 12:10,10 16:24 29:1 82:1 fourth 7:20 full 5:18 function 19:24 65:4 75:5 77:16,17,19 77:24 78:1 86:17 109:25 functional 101:11 functionality 78:3 functions 41:14 76:14 funded 8:10 further 103:24 104:15 112:14,15 113:13 future 24:11 95:12 99:6 G G 31:18 general 7:7 17:3 49:23 53:15 87:16 generate 26:12 generates 71:25	72:2 generation 7:19,21 9:12 15:16 90:4 107:3,14 generations 9:11 getting 61:14 90:24 91:8 98:17,19 give 6:13 10:2 12:19 45:23 51:14 57:8 given 35:8 49:8 60:20 65:2 78:23 91:19 93:24 113:11 gives 31:25 109:11 global 89:8 globally 15:22 71:8 go 5:21,22 8:11 29:3 30:7 47:23 48:11 61:25 65:9 67:1 74:1,9 80:4 87:23 95:2 98:8 98:25 100:16 101:2 104:4,17 112:10 goes 44:11 63:9 87:24 103:23 107:19 going 5:21 6:19 10:11 31:4 34:1 36:5 39:7,12 41:25 42:2 44:5 45:21 47:7 49:11 49:13 55:21 56:20 59:8 63:11 65:15 74:15 82:10 86:6 86:10 89:11,12 91:23 good 5:16,17 76:6 84:15,22 86:2 100:21,23 graduate 8:23 great 14:7 94:20 greater 95:16 greatly 14:6 ground 5:22 group 8:5,7,12
---	---	--	--	---

growth 95:11	HSS 53:7	identifies 50:19	78:25 83:3,7,11	individual 71:11
guess 61:14 77:8	HSSs 36:1,3	51:21,25 81:3,7	83:14,22 88:9,10	industry 13:20
89:24		identify 17:14	94:6,8,11,15	inefficient 55:6
H	I	21:23 28:7,22	95:18 110:5,9,12	57:25
half 12:10	ID 52:10	29:1 37:7 46:16	111:6,23 112:1,4	inferior 64:1,6
hand 43:21 80:20	IDC 11:19	50:22,25 51:6	IMSI s 36:18	inflexible 94:17
113:18	idea 22:10 107:20	57:2 66:11 69:8	inaudible 21:8 27:4	information 15:13
handle 21:5 30:5	ideas 90:20 92:4	71:6 96:4 98:12	include 25:1,6	26:23 36:18 45:19
63:1	identification 6:24	identifying 17:6	33:19 35:9 45:15	52:5,8,9 57:13
handled 19:7 21:4	10:9 31:8 33:24	71:11,14,20 79:13	68:11	58:7 68:12 72:19
21:6 22:8,15,16	36:14 47:12 65:19	97:4	included 46:17,18	73:4,17 85:17
handling 20:22	68:23 70:20 82:14	identity 42:23 43:4	79:12 80:16 93:10	88:6,15 89:14,15
38:6 101:24	108:15	50:12 51:20,25	includes 52:9 67:21	89:18,20 90:24
hands 55:24	identified 16:7	67:6,19,21,25	71:17,19 74:11	91:9 102:5,15,17
happen 78:10	21:19 30:11 45:13	74:10 79:12	86:13 100:14	103:5,17 110:19
happens 59:13	58:4 69:19	111:20	including 7:8 17:21	informed 23:8
hard 26:14,22	identifier 13:6,12	illustrated 32:13	25:16 30:2 66:23	initial 59:18
header 26:2	13:14,21,25 14:5	illustrates 35:4	100:8	Innovation 2:4
heard 5:25 9:20	14:8,16,17 15:2,5	image 103:18	incompatible 63:3	input 44:6 102:11
10:1,6	15:6,23 16:2,6,19	implement 20:13	63:13,14,15 64:2	102:12
hearing 11:13	16:22 17:3,8,11	61:2 63:22,23	64:11 97:14,20,22	inside 66:20
help 5:22	17:19,24 18:1,4	99:22	98:1,8 100:2	integrate 63:12
helpful 111:14	18:22 19:22 20:3	implementation	106:16	integrated 17:1
hereunto 113:17	20:16,17,19,24	58:1	incorporated 80:21	19:3 20:14 22:6
high 30:21	21:7,22 22:2,3,8	implemented 9:8	107:10,21,22	26:7,10,13 27:16
hold 80:6	22:18 23:23 24:2	9:14,17 13:24	incorporates 80:11	103:14
home 13:17 18:5,14	24:16 25:2,5,7	56:19 85:2	80:14,24	integrates 99:5
21:5 22:18 40:16	28:7,22,25 29:11	implementing	INDEX 3:1 4:1	integrating 20:9
46:9 66:12,18,21	29:18 30:15,20,24	26:20 60:9 62:17	indicate 31:1 49:17	integration 15:17
68:25 69:14 70:1	31:3,15,18,22,24	important 13:10	54:16	intended 22:15
71:13,14,17,21,23	32:1 36:22 37:11	81:5,8	indicated 24:15,25	intent 29:25
74:6,14 75:3,9,11	45:15 46:8,12	impossible 56:23	28:1 36:11 69:14	intercepted 13:22
75:19,20,21 76:1	48:20,22,23 49:1	IMSI 15:1,6,8,9,10	indicates 32:4,16	interception
76:13 77:18,23	49:2,4,19 50:1,14	15:20,22 37:15,20	33:13 111:23	103:21
78:6,12,25 79:21	50:18,25 51:6,20	38:15 39:17,21	indicating 10:21	interested 23:5,10
79:22 81:24 82:4	51:24 59:7 64:20	40:11 41:18,23	32:14,21 106:18	113:16
82:7 85:17 86:23	67:13,22 68:2,4	42:3,5,7 43:7,9,13	indication 32:9	interface 13:15
86:25 87:6,7,15	68:20,22 69:7	43:15 44:12,24	indicator 37:25	37:2 81:12
87:17,20 88:1,6	70:17 71:6,9,14	54:16 56:10,25	38:14 43:1,3	International 15:2
88:11,20,22 89:4	71:17,20 72:10	57:3 58:9,16 59:6	44:20 53:6,12	internet 23:11,13
89:9,12,18	73:21,22 74:3,6	67:18 68:24 69:9	56:14,16 60:5,8	23:15
hopefully 27:13	74:19 81:16,19	69:21 70:12,15,18	60:14,16 61:5,10	interpret 44:11
Hotel 2:4	82:3 83:16 84:3	70:23,24 71:11,16	61:16,21 62:13	56:24 63:6 89:1
hour 45:21	88:12,21	71:22 72:3,4,6,12	106:12 111:21	interpretations
hours 12:9,10	identifiers 16:3	72:14 73:3,9,16	indicators 38:3,7	57:2
HSF 56:24 63:6	21:8,15,17,19	74:11,14,16,23	38:11	interpreted 76:25
	36:8 37:1	75:3,12,16,18,25	indirectly 113:16	77:3

intervals 48:17 inter-operate 14:21 intimate 9:13 introduce 6:19 10:11 31:4 34:1 47:8 65:15 82:10 108:11 introduced 72:17 73:7 invent 19:9 25:13 26:6 invented 14:10,12 22:20 25:22 72:17 85:9 92:20 invention 13:2 14:4 14:24 23:2 24:3,9 47:17,24 64:24 67:9 73:2 84:23 93:7 98:19 103:13 103:23 inventive 19:4 22:12 60:16 72:18 93:24 98:12,23 inventors 27:3,12 27:14 invertible 43:18 investigation 80:1 involved 8:3 16:14 39:4 involvement 10:4 IPR 10:15 11:14 12:17 28:5 76:24 77:11 85:7 IPR2024-00702 1:7 IPT 27:24 issue 9:4 23:4 37:8 82:25 83:5,10,17 ITC 11:11 91:4 it'll 59:9 I-M-S-I 37:20 I.E 43:1	john.rhine@kirk... 2:9 joining 37:12 Joseph 2:14 5:6 jury 91:4	99:2 knowledge 9:13 43:8,14,19 60:20 known 13:19 14:25 15:8,25 16:1,3,7 17:4,10 19:13,14 21:15,17 25:17 55:23 84:25 93:9 93:10 96:18	94:1 95:22 96:4 96:15,21 longer 56:23 63:5 look 23:5 62:3 65:1 67:15 82:17 88:11 91:17 111:14 looking 23:4,6 52:13 74:10 79:11 84:2 85:19 99:2 105:18 lost 51:14 lot 26:15 65:8	meaning 26:14 33:12,18 45:6 107:24 means 32:19 33:2 53:16 79:23 110:23 meant 42:21 66:2 mechanism 26:19 mechanisms 17:6 media 103:17 meet 11:20 12:4,7 12:16 79:23 meetings 8:6,8,12 memory 38:21 39:1 39:6,7,9 mentioned 7:17 12:23 16:11,15 17:21 18:6 22:14 72:16 83:19,21 86:22 mentions 63:20 message 22:15 25:17 26:2 41:3,7 42:16 51:2,8 56:7 56:9 57:15,18 58:12,25 59:2,3,4 62:6 88:13,14 89:19 messages 19:25 25:14,16,20 26:5 67:11 109:13 met 12:9 method 38:5 48:21 49:1,9,9,16,17,21 49:23,25 50:18,21 50:22,24 51:6,20 51:21,24 52:1,10 55:4 57:22 60:6 60:13 61:17 62:15 62:20 63:1 64:8 64:19 79:7,20 97:3 methodology 13:5 61:3 83:13 methods 48:14 55:12 92:13 metrics 98:16
J	K	L	M	
jmicheli@mckoo... 2:14 Job 1:24 John 1:19 2:9 5:4	keep 39:11 111:12 keeping 25:20 key 14:17 20:16,17 20:19,23 21:1,8 21:15,17,19,22,24 22:1,2 24:19,23 25:1,4,6 34:6,7,9 34:10,18,23,24 43:8 46:6,8,9,11 46:14,17,21 48:17 50:24,25 51:5,6 52:10 67:12,12,22 68:10,19,22,23 69:2,3,6,10,11,12 69:18,19,20,24,25 70:4,7 75:8 81:24 82:4,7,25 83:5,10 83:12,16,22 84:17 92:16 99:13,17,20 99:23,25 100:4,11 keys 21:20 34:10 34:11 48:13 49:8 49:12,14 68:24 92:15,18,25 93:3 93:4,6,8,9,10 99:18,23 103:8 KIRKLAND 1:20 2:10 knew 84:22 Knocking 94:25 know 6:9 10:19 27:20,22 32:19 33:1 52:6 54:9,10 54:18,23,25 55:15 55:18 56:18 57:19 58:10,14 59:5,8 62:9 63:16 88:1,5 90:18,20,25 91:5 98:20 100:5 knowing 53:16,21	lack 64:15 lapse 49:8 larger 35:10 laudable 108:2 layers 9:16 leading 9:11 left 43:21 legacy 48:9 65:5 97:8 103:1,4 Lenovo 1:5 5:5 Lenovo's 11:13 let's 62:4,5 69:16 104:17 level 30:21 limitation 31:1 35:23 42:14 76:25 limited 48:5 77:12 limiting 33:21 80:2 94:21 line 44:5 47:17,23 48:11 52:14 104:4 114:2 lines 51:16 52:7,22 111:14 listed 11:10 listing 31:23 literally 54:7 little 5:21 51:4 53:25 86:7 98:20 LLP 1:20 2:10 LM 1:9 located 18:14 location 86:17,18 long 12:7 51:4 70:16,23 73:22 83:16 93:3,25	Mahon 1:12 2:1 3:3 4:4,5 5:9,20 7:2 10:14 31:11 34:5 100:22 104:16,23 108:8,18 113:5 114:24 maintained 107:10 majority 14:5 making 23:20 55:23 78:11 manage 99:19 managing 99:12,16 MAR 4:3 Mark 1:12 2:1 3:3 4:4,5 5:9,20 113:5 114:24 marked 4:3 6:20,23 10:8,12 31:7 33:23 34:2 47:8 47:11 65:16,18 82:11,13 108:12 108:14 materials 112:11 matter 62:19 64:1 64:10 matters 64:17 73:13 106:7 MCC 88:7,23 MCC/MNC 85:23 McKool 2:15 5:7 mean 16:9 49:25 64:6 97:20,20 110:24	

Micheli 2:14 3:4 5:6,6 45:20 61:7 61:19 64:4 78:15 79:15 86:2 91:14 98:14 104:17,22 105:3 106:6 107:2 107:4 108:3 112:15 middle 100:7 mid-field 98:13 mind 28:17 31:11 34:14,25 36:4 39:11,23 42:17 45:9 51:11,16 52:13 56:20 86:11 108:21 missing 67:24 mistakes 10:20 MME 69:8 75:3,9 75:11,19,21 76:1 76:13,22 77:18,23 77:23 78:7,13,19 78:25 79:1,8 MNC 88:7,24 mobile 15:2 36:17 70:19,19,20 79:4 84:15,23 93:9 modern 14:21 94:18 Monday 12:10 morning 5:16,17 motivated 24:5 65:13 99:11 motivation 64:14 64:16,22 moving 34:25 43:20 MSIN 71:18 85:13 85:16,22 multimedia 48:3,6 48:9 66:24 97:7 multiple 17:14,20 17:23 21:20 32:23 36:1,3 62:21 63:2 64:2,11 68:24 89:4 92:11,12,15 92:19,25 93:4,6,8	93:10,17 94:13 95:15,21 97:4 99:13,16,20,22,25 103:17 106:9,13 106:16,21 multi-way 66:23 MYMO 8:24 M-A-H-O-N 5:20 N Nair 4:8,12 34:5,15 34:17,21 35:3,19 36:4,7,12,16,21 36:23,25 37:6,10 37:14,24 38:2,5,9 38:11,18,24 39:14 39:16,20,23 40:23 41:17 42:17,18,23 43:21 44:5,11,15 45:12 54:14,22 55:7,8 56:4,5,6,12 56:13 58:1 60:12 60:25 61:24 62:12 62:13,18,22,24 63:9,12,13,15,17 63:19,24 64:14,19 64:23,25 65:24 66:1 67:8 80:4,8 80:10,10,14,20,24 81:3,10,22 82:5,9 86:7,16,17,19,24 86:24,24 87:4,18 89:1,17 94:6 99:11,12,24 100:8 100:10,13 105:6 105:11,14,18 106:8 108:18,25 110:5,9,11,20 111:19 Nair's 38:13 46:4 53:6 55:14,22 60:4,8 61:5 62:17 63:3 64:1,6,10 94:16 100:2,3 105:9 106:12 110:1 name 5:18 72:23	73:13 narrow 54:5 narrower 53:25 necessary 94:14 need 6:9 24:23 25:4 34:22 45:18 46:25 95:22 96:4,15,22 97:1 98:15,16,20 99:24 needed 46:6,21 68:12,23 needing 96:5 needs 46:16 96:2 nefarious 13:22 network 8:17,22 13:13,16,17 14:19 14:22 16:13,14 18:3,5,12,14,15 18:15 20:12 21:2 21:5 22:9,16,17 22:19,25 23:6,14 25:9,23 27:16 35:13,17,24 37:13 38:14 40:16 42:15 46:9,15,16 47:22 48:4,9 50:7 55:15 57:10,14,17,19 58:20,22,25 59:3 59:8,16,18 61:12 65:4 66:11,12,18 66:19,21 68:25 69:1,9,14 70:1,5 70:19 71:7,13,14 71:17,21,24 74:6 74:14,20 75:20 76:12,13,14,21,22 76:23 77:2,12,15 77:17 79:9,21,22 81:24 82:4,7 85:4 85:8,17 86:23,25 87:3,6,8,9,15,17 87:20 88:1,6,11 88:12,20,22,23 89:3,8,9,18 94:7,9 94:11 95:18 96:2 97:13,16 112:3 networks 23:1,7,16	23:19,20 25:18 37:3,7 47:20 48:1 65:6 67:4 70:23 70:25 81:6,9 89:4 89:12 90:5 95:12 never 29:17 new 15:14,16 20:10 20:13 37:12 94:5 non-obvious 90:1 90:16 91:13 non-obviousness 90:10 92:3,9 non-voice 104:1 normal 59:12 Notary 1:24 2:3 113:3,22 notified 52:19 novel 13:1 14:23 16:23,25 17:2,25 19:20 20:15,16 22:9 60:22 93:1 95:13 novelty 13:3 16:16 18:6,10 20:4,7 null 24:16,19,21,24 24:25 28:12,13 32:4,7,14 43:22 43:24 44:1,6,16 44:21 45:2,5 110:2,3,15,17,21 110:24 111:2,3,4 112:6,8 number 17:12 33:21 70:21 80:18 90:21,22 91:5 92:18 numbers 35:10 36:18 N.W 1:21 2:10 O objection 61:7,19 64:4 78:15 79:15 91:14 98:14 106:2 obvious 91:25 obviously 11:7,13 14:13 26:25 57:25	73:5 90:7 91:23 occurring 57:9 77:18 office 1:1 113:18 Oh 66:2 okay 10:23 23:22 28:19 29:22 31:13 31:25 32:16 34:14 34:16 35:2 36:24 38:17 39:13,24 42:20,22 45:11 47:2,7 51:15 52:13,15 53:4,19 54:8,11 56:22 60:4 62:18 63:4 67:17 69:17,23 74:2 80:4,6,9 82:22 84:14 86:12 87:1 88:9 99:9 100:16 112:12 older 50:7 operator 20:12 70:5 81:24 82:8 96:3 operators 21:2 operator's 89:11 opined 91:9 opining 85:7 opinion 12:25 16:23 22:21 28:6 34:17 42:4 43:3 46:3 48:5 54:11 55:3,6 68:14 73:10 77:10 78:2 89:25 90:15 97:12 97:14 99:24 100:10 110:1 opinions 28:4 76:24 79:25 option 54:13 56:2,3 56:8,8 options 92:23 order 45:18 49:14 78:10 99:25 ordinary 18:25 24:4,8 43:6,11 44:19 62:14 65:1
--	--	--	--	--

65:12 76:8 84:1 88:25 93:22 96:10 99:10 109:17 organization 107:5 107:6 oriented 47:21 48:2 48:7,10 50:3,7 65:5 67:5 77:5,15 97:6 original 11:10 output 44:7 outside 19:18 50:16 60:2 overall 22:11 overhead 103:5 owner 1:10 2:1,13 5:7 6:17 owner's 11:15	81:10,14 89:21,24 99:7 100:6,7,15 105:9,17 112:11 parameters 68:9 68:10 paraphrasing 90:6 Pardon 52:7 part 8:9 13:9,9 14:4 16:15,17 17:2,9 20:6 28:2 37:15 41:10,12 49:10 50:1,12 61:24 67:19 73:1 73:8 74:4 85:1 86:22,23 87:2 88:3,9,10 particular 13:10 17:18 18:21 21:24 23:3 26:13,16 43:8,14 50:22 53:21 83:8,14 particularly 17:25 parties 36:19 113:14 Partnership 107:3 parts 26:4 party 1:16,19 103:21 passed 18:3 26:23 patent 1:1,3,8,10 2:1,13 4:5,6,7,9 4:10 5:7 6:17 9:5 11:15 12:22 14:24 15:20,25 16:4,10 16:25 17:4,17 19:9,11,15 21:16 22:1,22 24:4,10 24:14,25 25:13,21 26:6 27:3,12,14 28:11,13 29:14,16 29:17,22,24 30:10 31:5 40:24 41:5 42:11 46:19 58:3 58:10,13 66:13,17 68:15 76:11 77:25 78:3,8,9,14,21 84:24 85:5,9 87:4	90:1,10 91:13,17 91:19,21,22 92:21 93:2,16 96:4 105:14 110:11 patents 11:7 90:18 90:25 91:3,10 patent's 13:1 path 101:5,5,17,18 101:20,23 paths 101:4 Pause 47:5 86:4 95:4 100:19 104:20 pending 6:10 Penn 2:3 Pennsylvania 1:20 2:3,4,10 113:1,4 people 18:8 perform 40:20 55:2 59:9 62:4 75:4 109:25 performed 60:19 79:20 performing 19:16 40:12 41:2,4 57:20 60:24 75:24 76:3,15 77:20 109:22 performs 40:14,21 76:9,13 78:1 period 31:18,18 permanent 13:6,11 16:1 18:4 20:3 21:7 22:17 23:23 70:17 73:21,22 81:16,19 82:3 83:15 84:3 permission 8:11 permit 8:14 22:16 permits 13:13 permitting 13:11 person 18:25 24:4 24:8 43:6,11 44:19 62:14 64:25 65:12 76:6,8 84:1 88:25 93:22 96:9 99:10 109:17,19	perspective 62:12 93:22 petition 11:13 petitioner 1:7,17 2:8 5:5 phone 66:24 phrase 43:24 112:8 pictured 109:4 place 113:8 plane 13:12 23:13 23:14 26:1,1 65:4 65:6 platform 15:23 play 18:13 59:11 playing 50:8 please 5:18,24 6:2 6:5,9 31:12 36:4 42:19 43:10 47:3 51:23 64:9 65:24 80:4 95:10 105:5 111:12 112:10 plus 34:12 point 10:25 13:16 15:7,11,11 54:22 55:7 73:6 77:16 99:3 pointing 63:5,14 64:15 100:13,15 110:25 points 26:17 populated 25:10 portion 25:19 74:11,12 portions 25:20 POSITA 24:21 29:25 33:13 34:21 39:2,8 43:16 44:3 44:23 45:14 46:13 62:12 69:4 84:1,5 85:16 88:4 109:24 110:18 112:9 possibilities 28:23 29:1 possibility 63:12 possible 28:2 29:19 29:23 30:18,23 32:23 57:2 63:6	63:14 post 11:12 post-hearing 11:16 potential 28:7 PP 8:5,7,8 27:25 28:2 70:23 practical 85:18 preamble 79:19,24 80:2 predates 10:3 preferred 106:12 preliminary 11:15 preparation 12:3 prepare 11:4 12:4 12:8 prepared 12:19 preparing 11:21 12:13 present 12:13 25:3 25:11 presents 62:8 presume 112:4 preventing 55:21 prevents 82:1 previous 13:23 59:25 98:25 previously 4:3 6:20 6:23 10:8,12 18:23 31:7 33:23 34:2 47:8,11 65:16,18 82:11,13 108:12,14 printing 113:10 prior 11:8 15:25 16:4,8 17:10 19:13,15 21:16,17 21:19,23 22:3 23:7 25:18 27:17 27:23,25 85:6 priority 105:12 privacy 22:23 36:7 36:13,25 37:24 38:2,7,11,13 42:23 43:1,3,4 44:15,20 46:21 53:6 56:14,16 60:5,8,14 61:5,10
---	---	---	--	---

61:16,20 62:13 81:4,8,12 106:12 111:20,20 private 34:6,9 46:6 46:11,14,17 69:2 69:10 99:13,17,23 probably 55:1 87:14 problem 13:18 15:5 18:7,20 36:16 37:2,5 47:18,24 58:4 60:23 63:19 67:2 83:19 93:20,25,25 94:5,6,14 problems 14:6 65:9 107:13 problem's 99:3 procedure 2:2 60:10 97:15,19,23 98:9 procedures 59:20 98:5 PROCEEDINGS 5:2 process 22:24 37:12,14,16 processing 19:7 38:3,8,21,25 processor 102:11 produced 10:25 product 8:16,18 products 8:19 progressed 7:19 Project 107:3 pronounce 9:25 proper 59:10 69:2 88:23 proposals 15:7 27:25 107:15 propose 27:15 61:12 proposed 27:20 28:1 75:13 85:5 proposing 61:15,16 61:20 protect 13:25 14:4	14:15,20 15:1,3 16:1 22:17 protected 14:6 44:25 46:15 103:20 protecting 13:5 21:6 22:23 36:21 50:11 protection 13:11 13:14 14:7 18:4 22:23 36:13 protocol 9:12 25:23 32:20,21 33:3 protocols 7:19,21 7:25 8:2,25 9:7 33:9 59:20 98:6 provide 15:4 20:9 20:21 30:1 81:11 94:23 provided 14:7 18:16,17 20:6,7 28:5 79:25 88:6 93:21 99:4 103:19 111:23 112:5 providers 89:5 provides 26:19 62:22 64:21 77:24 82:6 94:22 95:11 99:5 109:14 providing 11:18 14:13,15,17 20:24 65:25 66:6 83:11 92:5 provisional 4:12 105:12,14,19,22 105:25 106:5 108:18,24 109:3 109:10,11 110:1,4 110:20,22 111:5,7 111:13,17,19 PTAB 11:10 public 1:24 2:3 14:17 20:16,17,19 21:8,15,17,19,20 21:22,24 22:1,2 24:19,23 25:1,4,6 34:6,9,18,23,23	46:8,9 67:12,21 68:9,19,22,23 69:3,6,11,18,24 69:25 70:4,7 81:24 82:4,7 83:12,22 92:15,16 92:18,25 93:3,4,6 93:8,9,10 99:13 99:16,18,22,22,25 113:4,22 Publication 4:7,10 public/private 20:23 21:1 69:12 75:8 99:20 100:4 100:11 published 108:25 pull 56:10 purport 93:16 purported 58:3 purpose 30:1 50:15 53:5 69:6 purposes 13:22 89:13 put 11:9 14:12 18:10 26:15 32:12 61:3 putting 19:4 22:10 P.m 112:18	reading 29:15 85:16 really 92:1 reason 6:13 57:17 57:19 63:15 114:2 reasonable 87:8 102:6 recall 10:1,5 11:1 12:1 27:17,17,22 80:3 105:4,8 106:10 receive 57:13,18 received 41:3,7 58:15 59:2 receiver 49:7 54:16 56:18 101:21 receives 40:17 89:16 receiving 46:5 101:16,22 recognizes 36:25 37:6 recollection 64:21 record 1:18 5:19 47:5 86:4 95:2,4,6 100:17,19 104:18 104:20 113:11 recorded 113:9 REDIRECT 3:4 108:6 reduced 113:10 reference 47:15 80:11,21 84:7 101:1 referenced 33:14 referring 16:21 54:1 68:6 108:19 reflected 105:19 reflects 90:2 regard 19:21 80:1 regarding 81:23 rejected 55:19 rejection 59:3 relate 102:24 related 9:19 32:23 68:9,10 relates 36:7,12	47:17 65:24 66:5 66:7,13 79:4 81:15 relative 113:13,14 relevance 11:16 relevant 9:3 11:6 relies 46:4 rely 96:23 112:13 relying 64:18 90:9 90:11 remember 10:6 11:3 repeat 43:10 51:3 51:23 rephrase 66:3 report 11:8 85:14 REPORTED 1:23 reporter 2:3 3:6 6:3 9:22 21:10 27:6 35:15 37:18 82:19 93:13 106:25 113:3 represent 29:7 representing 17:23 represents 17:12 request 38:6 42:1 45:15 57:10 58:23 59:1,16,18 87:19 87:22 88:17,19 89:16 requesting 74:18 require 17:17 29:23 41:5 46:11 78:3 required 43:19 68:14,17 95:17 requirements 20:12 requires 34:6 42:13 43:7,13 46:8 78:4 requiring 41:13 77:1 research 7:22 8:9 8:21,23 9:2,10 resources 26:16 38:4,12 54:24 56:11,13 60:24
---	---	--	---	--

62:9 63:21,25 respect 26:21 59:15 59:24 77:4 87:5 103:13 respond 6:10 response 11:15 67:19,21,25 74:10 79:1,12 responsibility 88:3 result 38:12 results 93:17 retained 4:15 review 11:23 105:14,17,20,23 106:1 reviewed 11:8 112:11 reviewing 111:9,12 revise 27:9 Rhine 1:19 2:9 3:3 3:4 5:4,4,15 6:19 7:1 9:24 10:11,13 21:12,14 27:9,11 31:4,10 34:1,4 35:18 37:21 45:23 46:2 47:2,7,14 61:13 64:7 65:15 65:21 78:18 79:17 82:10,16,21,23 84:13 85:25 86:6 86:9 91:20 93:15 95:2,6,9 98:18 100:16,21,24 104:15 106:2 108:8,11,17 111:11 112:14 right 12:2 23:12,17 25:22 28:12 32:8 38:22 39:1,6 45:15 46:6,9,22 51:8 61:14 69:21 69:24 71:25 80:10 80:20 81:12,17,20 87:3 91:21 93:7 94:10 102:25 105:9 107:5 109:1 110:6	roaming 18:15 21:3 66:10,10,11 66:13,15 75:13 87:11 88:5 rolled 20:11 rotated 69:24 route 88:14 89:19 routed 88:22 rules 2:2 5:22 Ryan 45:20 S satisfy 79:14 save 53:6 54:2 saves 38:3,7 saving 54:24 saw 10:23 saying 35:11 54:1 54:14,23 57:14 63:11 72:25 73:3 73:13 77:14 111:1 says 43:1 44:6,15 80:21 81:3,10 83:15 101:10 103:12 scale 98:11 scant 64:21 scenario 57:8 scheme 14:16 16:3 16:5,19,22 17:3,8 17:11,12,15,18,24 18:1,21 19:22 20:2,5 21:25 22:7 24:16,17,25 26:7 26:10,14,22,24 28:3,6,11,12,13 29:11,18 30:15,19 30:24 31:2,14,17 31:22,24 32:1,4,8 32:15 33:8,11 34:5 43:14,18,22 43:25 44:1,6,21 45:2,6,13 46:23 48:20,23 49:1,3 49:18,22,24 50:13 50:19 51:1,7 52:16,19 53:22	55:5,16,18 56:19 57:7 58:15,19 59:7,9 60:17,18 60:21 61:22 64:20 68:1,4,9,10 70:7 79:13 83:4,8,14 83:24 85:2 95:20 95:24,25 96:1,5 96:13,21 97:9 98:4,13,21 110:2 110:3,15,21 111:2 111:3 schemes 14:20 17:6 20:10 24:15 27:1 28:8 29:12 30:6 32:24 33:14,16,17 33:19 62:21 63:2 64:3,12 92:11,13 92:19,24 93:18 94:13 95:16,22 97:4 106:9,13,16 106:21 scope 106:2 seal 113:18 second 7:20 51:14 74:19 80:6 82:2 89:25 101:12 secret 67:12 69:19 69:20 secrets 68:12 section 64:13 82:17 82:24 83:2,9,24 84:4,9 85:14,20 103:23 112:11 secure 24:5,10 52:24 security 7:8 8:1,13 8:25 9:7,14 23:9 36:7 66:22 81:5 90:4 96:24 see 29:8 35:22 39:25 40:6 42:24 44:9,13,14,17 56:3,9,25 57:4 72:12 80:15,16,17 80:18,18,23 84:17 85:3 87:10 90:7	91:17,24,25 100:9 103:24 104:8,13 106:5 111:21 seeing 27:23,25 55:12 select 19:24 selected 40:18 41:1 41:6,15 send 41:20 sender 49:7 sending 41:11 52:23 59:17 87:21 sends 39:20 41:17 78:25 87:18 88:16 sense 62:25 86:1 sent 13:16 36:19 67:18 88:20 sentence 89:24 separate 34:11 101:23 server 18:13 19:10 19:12,13,14,17 33:1,4 40:3,9,13 40:13,16,23 41:6 41:9,9,11,12,15 46:20 58:14 59:5 66:18,20 74:24,25 75:2,19,20,22 76:2,4,5,9,10,18 76:20,25 77:2,12 77:13 78:7,13,21 79:9,20,21 86:17 98:22 106:3,4 109:8,18,20,25 service 103:14 set 44:24 48:17 49:6 98:4 112:3 113:17 setup 65:9 103:3 shared 68:11 SHEET 114:1 shorter 84:17 shorthand 53:19 shortly 45:22 show 30:18,23 109:4,5,6 showing 79:7	101:23,24 102:10 shown 35:6 68:5 87:21 101:13 shows 30:15 41:25 85:22 109:14,22 SIDF 18:13 20:1 75:5 76:14,21 77:20,24 signal 41:25 101:5 101:9,20,23 102:1 102:5,14,20,22 signaling 8:25 49:10 signals 39:5 102:25 104:1,2 similar 108:25 similarly 40:21 simple 55:25 simplicity 35:7 simply 57:6 Simultaneous 84:11 single 34:9,23 35:4 35:5,23 36:2 95:19 100:4,8,11 100:14 sir 5:17 sit 10:17 sits 40:16 sitting 66:20 situation 75:13 97:25 110:9,12 size 84:17 sketch 30:21 skill 18:25 24:4,8 43:6,11 44:19 62:14 65:1,13 76:8 84:1 88:25 93:23 96:10 99:10 109:17,20 SLF 34:18,22 35:4 35:6,19,22,23 36:2 40:5,8,11,22 41:1,18,21 53:7 56:24 63:6 86:14 86:16,20,21,22 87:22 88:17,19
--	---	---	--	--

89:9,10,16,20 100:8,14 109:22 Smith 2:15 5:7 solution 14:2 18:16 18:23 58:3 60:9 61:10 62:22,23 63:22 64:2,6,11 81:23 82:1,2,25 83:21 84:2 92:6 93:24 94:19 97:12 99:2,4 solutions 28:3 81:11,15 82:6 92:5 107:14,16 solve 18:9,19,22 37:4 58:4 60:23 63:19 93:19 94:14 107:13 solved 13:18 14:5 18:23 65:10 93:25 solves 62:1 94:6 95:22 solving 18:7 36:16 94:5 sorry 14:14 39:11 42:21,21 52:6,7 52:17 53:23 66:1 66:2 69:7 73:12 74:16 76:6 86:21 110:8 sought 94:1 sounds 95:15 speaking 84:11 specific 13:8 41:13 49:14 58:6 66:7 80:17 90:14 94:9 97:21 98:4 specifically 7:17,23 9:8,15 15:17 16:18 20:20 35:21 35:25 36:1 38:14 48:2,15 50:8,10 54:4,15 60:15 68:8,17 83:2 85:15 96:25 99:19 103:12 104:13 112:3	specification 29:13 52:5,8,17,24 102:15,17 specifics 98:16 specified 80:19 speculation 91:15 speed 55:8 62:25 spent 7:22 12:13 sponsors 8:11 SS 113:2 staff 11:16,19 staff's 11:12 standard 8:4 27:21 84:21 90:2,11,13 90:16,19 91:1 92:2 107:10,12 standards 8:8 92:22 107:14,17 107:21,22 start 8:19 12:23 started 7:15 87:1 starting 47:16,23 48:11 52:14 104:4 state 2:4 5:18 29:5 36:1 37:9 53:5 66:25 81:13 stated 46:4 113:8 statement 84:19 Stater 2:3 states 1:1,5 29:8 35:5 41:8 52:11 52:21 81:7 89:5 stating 58:17 stenographically 113:9 stream 98:3 streams 101:25 stress 91:24 strike 27:12 58:12 74:16 86:21 89:3 110:8 112:13 string 17:16,21 23:24 32:11 strings 17:21 strong 26:21 structure 103:4 structured 98:5	structures 26:2 29:6 students 8:23 SUBI 81:20 submit 107:15,15 subscriber 15:2 36:13 70:20 71:9 71:15 86:18 subscription 36:17 37:1,11 71:21,23 81:4,7,16,19 83:16 84:3 substantially 108:24 successful 54:18,19 59:22 SUCI 9:20,24,25 10:2 13:7,8 14:3,9 14:9,11,14,20 15:18 16:12,23 18:1,2,11,22 19:4 20:1,25 22:6,11 22:14 25:1,3,8 30:13,22 32:7 41:10,11 42:11 44:24 45:13 50:1 67:24 71:25 72:18 73:8 suddenly 63:11 sufficiently 12:19 suggest 27:3 suggesting 60:12 60:13,25 62:18 suggestion 27:23 Suite 2:16 SUPI 14:14,23 15:9 15:10,21,24 23:22 23:23 39:15,18,19 40:14,17 44:7,12 70:10,11,14 71:8 71:13,19 72:2,4,6 72:11,13,14,23,24 72:25 73:4,7,9,11 73:18,20 81:23 82:6 83:6,10 85:4 85:8 SUPIs 83:1	support 30:4 68:3 90:14 109:9 supported 105:22 105:24 106:5 sure 20:18 21:12 24:7 27:18 51:5 51:24 55:23 98:15 98:17 surprising 93:17 94:2 switch 49:7 switched 44:16,21 sworn 5:10 113:6 system 9:18 14:22 15:16 20:21,25 22:25 24:12 30:4 35:10,12 36:9 40:12 41:4 48:18 48:22 50:23 55:14 55:22 56:4 62:1 62:17 86:7 93:1 94:10,16,19 96:19 97:8 98:10 100:2 100:3 101:12,14 103:1,4 108:1 systems 7:7 20:8 23:11 93:11 96:22 S-U-C-I 9:24 S-U-P-I 14:15 T table 107:25 take 6:3 26:23 45:21,24 47:2 54:21 67:15 taken 2:2 94:21 95:14 113:7 talk 12:22 28:4 53:20 86:6 99:19 109:12 talking 39:3 70:24 79:16 teach 50:3 99:12,16 99:24 teaches 34:17 37:10 38:2 48:19 51:19 52:16,23	56:12 63:3 67:11 67:18 68:19 69:18 69:23 84:14 85:12 92:10 110:5 teaching 46:5 48:2 58:1 63:10,17 technical 22:21 23:3 107:16,24,24 technically 32:12 technique 13:4 20:13 26:11,25 48:8,12 55:9 58:7 84:25,25 98:7 techniques 9:14 13:23 22:20 23:9 25:16 69:5 technology 8:24 9:4 107:9 telecommunicati... 22:25 24:12 telecommunicati... 7:10,16 13:20 79:8 90:4 TELEFONAKTI... 1:9 telephone 103:19 tell 5:24 55:25 60:17 92:1 98:21 telling 53:7 62:1 temporary 15:4,5 term 10:5 14:3 16:18 17:9 19:12 19:14,17 20:19 39:19 42:23 49:23 53:14,25 54:5 55:1 70:16 72:11 72:16,20 73:5,22 83:16 91:2 103:25 110:22 112:8 termed 103:3 terminology 73:9 73:12 terms 19:16 32:9 42:15 62:24 86:17 93:19 94:18 102:1 109:9 110:23 test 53:9
--	--	--	---	---

tested 91:24	97:3,6,10,21 98:7	54:17,17,25 55:11	19:1 24:7,22	50:11 51:22 52:1
testified 5:11	101:1,8 102:2,3,8	56:2,7,9 57:6,21	29:25 31:21 34:22	59:1 66:12 67:2,6
testify 12:14 113:6	102:24 103:1,10	57:23,23,24 69:9	39:2,8 43:7,12,16	67:19,21,25 70:17
testimony 6:14	103:12 104:5,10	trying 18:8,19 37:4	44:3,20,23 45:7	71:10,11,23 74:10
11:19 113:11	Togawa's 47:17,24	50:2 53:8,11,17	46:14 61:9 76:9	75:7 79:11 88:5
text 13:9	50:18,21,24 51:5	53:17,20,23 54:2	85:16 87:15 96:10	96:2 101:4,4,8,17
texts 36:20	51:24 97:12	54:4 59:25 60:23	97:24 109:24	101:19 102:1,4,7
Thank 104:16	101:10	61:2,3 62:10	understanding 9:7	102:18 103:10,15
108:3 111:18	top 52:4 80:20	63:19 65:9 73:14	9:9 18:24 19:2,6	104:6,10,12
theory 59:12	total 35:12 76:20	89:10 107:13	29:10,12 30:4	users 13:6
thing 43:4 44:1,4	touch 42:16 65:7	turn 36:23 37:22	33:6 61:21 62:11	user's 13:21 14:8
101:9 109:9	TR 4:11 80:11,14	46:3 53:2 69:16	77:11 88:4 92:7	21:7 24:1 36:21
things 50:5	80:18,21,24 81:3	80:8 82:16 84:8	105:11	50:12 56:10
think 10:22 23:8	81:10,22 82:5,24	89:21 99:7 105:5	understood 5:25	uses 18:1 22:1
51:13,14 54:4	83:15 84:4,14	turned 53:8 71:1	6:8 11:19 34:20	26:11 31:17,18
71:1 95:21 110:20	85:12	turning 28:17	49:23 69:4 70:3	32:8 42:23 69:8
thinking 25:24	TRADEMARK	31:11 34:14 36:4	70:16 83:18	utilized 32:24
third 7:20 27:13	1:1	38:16 39:23 42:17	109:16,19 110:17	92:24
33:10 36:19 89:24	traffic 36:3 47:19	45:9 51:11,11,16	unencrypted 25:21	U.S 1:8 4:5,6,7,9,10
89:25 103:21	67:3	52:4 59:19 60:4	36:17 44:8 45:4	90:6
107:3	transmission 39:5	81:10 108:21	74:12 112:4,5,7	
thought 60:3	46:13,18 50:8	two 9:16 12:9 28:7	unexpected 94:4,4	V
thousands 90:22	57:21 65:11	29:8,11,19,23	unique 15:22 71:8	vague 79:15 90:20
three 9:16 12:9	transmit 42:11,14	30:5 34:10,11,13	United 1:1,5 89:5	valuable 90:3
82:1	57:21 58:25	45:23 50:4 55:11	unsuccessful 13:25	value 17:15 32:4,8
time 10:1,23 11:2	transmits 41:23	55:12 57:2 65:2	18:20	32:14,16 33:6
14:23 15:7,12	58:19 104:7	65:14 66:23 86:19	update 48:13 70:7	62:3 107:24
24:3,9 27:13 38:3	transmitted 20:1	100:13 101:3,25	updated 69:24 70:2	values 29:19,23
38:8 48:17 49:8	26:5 41:20 74:23	109:15	updating 70:4	30:18,23 32:1,22
53:6,8 54:2,23	89:18 103:20	TX 2:16	use 16:22 20:4	33:7
55:16 62:16 73:6	transmitter 56:18	type 20:5 39:4,9	23:15,19,19 24:19	various 9:11 14:19
84:16 85:9,25	101:21	typically 43:18	32:7,11,14 38:3,7	17:5,16 18:8,18
92:21 93:1,4 94:1	transmitting 36:8	typos 10:19	38:13 39:17,18	verbally 6:2
113:7	42:5,7 56:4 57:9		41:9 43:17 51:21	versa 54:21
times 98:25 110:14	75:2 98:2 101:15	U	52:1 53:19 56:14	version 80:11,18,25
today 5:23 6:13,16	101:22 103:8	UE 32:19 33:4 35:6	56:16 61:20 62:15	versus 65:10 104:2
10:18 12:5,14,20	104:5	37:11 38:18,20,25	62:23 63:1 70:6	vice 54:20
110:14	trial 1:3 54:25 55:2	39:20 41:22,25	70:11 72:23 73:6	video 103:19
today's 12:3,8	55:3 60:6,12,24	42:4,7,11,12,13	83:20 93:3,6,9	view 18:24 19:1
Togawa 47:15,21	60:25 61:3,6,17	55:11,17,18 56:4	94:8,13 95:19,24	visited 66:19 69:8
48:2,5,7,10,11,12	62:15,19,20 63:1	57:6,9,13,20	95:24 96:17 98:21	78:19 79:1 87:2,6
48:15,19,21 49:5	63:17,21,25 64:8	58:10,11 71:25	98:22 99:18,25	87:9
50:1,5,10,13,17	64:10,18 106:8,15	81:4,17,20 85:13	100:8 110:22	visiting 13:15
50:23 51:9,10,12	tried 63:8	88:2 89:15,19	111:1,20 112:7	18:15
51:19 52:11,11,16	true 39:6 113:11	UEs 37:12	user 14:18 23:23	Vitae 4:4
52:23 64:14,23,25	truth 113:6	Uh-huh 58:21	25:9 32:25,25	voice 23:16,20 48:3
65:5 92:10,12,16	try 6:5,6 26:16	understand 5:23	36:8 38:6 39:3,9	48:6,8 50:6 97:7

101:5,9,17,20,23 102:1,4,11,14,20 102:21,25 103:17 103:18 104:2,14 vs 1:8 vulnerable 14:1 96:19 V1.1.0 4:11	111:9 113:5,12,17 word 31:17 32:7 80:16 109:15 111:2 words 75:15 83:20 96:17 111:2 work 7:18 8:1,9,10 8:13,23 13:12 57:22 97:19 107:12 worked 99:1 106:8 working 7:16 8:5,7 8:12 10:25 12:16 93:23 96:24 109:13 works 54:9 55:12 56:3 94:10 world 107:7 wouldn't 10:2 55:18 62:15 63:16 79:14 wrong 52:6 66:4	1004 4:7 33:23 34:3 36:5 80:5,6,7 86:8 105:5 109:1 1005 4:10 65:16,18 66:3 1006 4:9 47:9,11 1007 4:11 82:11,13 1008 4:12 108:12 108:14 10208 1:24 105 3:4 108 3:4 4:12 100:6 11 36:6,11 113 3:6 12 1:14 2:5 1200 2:16 1301 1:20 2:10 131 53:3,5 60:4 132 56:20 57:12 58:5 14 104:4 16 28:22 104:4 17 51:16 111:14 18 52:7 111:14 19 67:1 74:1,15 108:22,23	28 81:10 29 47:23 3 3 30:10,18,21 48:11 68:5,7 3G 8:5,7,8 27:25 28:2 37:3 70:23 70:25 71:3,4 3GPP 4:11 90:3 92:22 98:5 106:23 107:2,11 112:13 30 7:15 81:14 300 2:15 31 4:6 32 63:4 33 4:7 33.899 4:11 80:11 80:14,18,21,25 81:3,11,22 82:6 82:24 83:15 84:4 84:14 85:12 34 52:14 35 42:17 376 82:17 378 84:8 38 34:14,20 4 4 31:11 33:11 67:15 68:5,7 69:15 74:9 79:7,11,22 4G 23:1,7,9 37:3 76:12,17,23 77:17 4-bit 28:22 41 42:21,22,24 42 39:12 43:20,24 105:9,17 43 37:22 47 4:9 5 5 3:3 35:1,1 43:21 66:25 68:5,7 5G 7:12,14 8:3,16 8:21 9:1,2 14:22 19:2,20 23:1,6,10 23:11,14,16 27:16	27:21 32:21 37:7 65:4 76:12,14,21 76:22 77:1,5,12 77:15 81:5,9 84:21 85:4,8 89:3 90:2,5,11,13,16 90:19 91:1,10,13 92:2 94:7,9,11 95:18 97:13,15 5.7.4.15 82:17,21 5.7.4.15.2-1 85:19 50 30:7 38:16 101:15 55 28:17,21 30:3 69:16 56 29:3 57 34:25 35:3,5,11 59 89:21,24 6 6 4:4 39:23 40:5,10 40:23 41:17,21,22 41:25 86:10,12,13 87:18 108:21,23 108:24,25 109:3 111:12,16,17 60 101:16 608 39:25 610 40:5 65 4:10 7 7 47:17 80:8,10 70 101:5 75201 2:16 8 8,005,219 4:9 8:58 1:15 2:5 80 101:6 817 9:5 12:22 13:1 13:3 14:24 15:11 15:20,25 16:4,5,7 16:10,12,16,25 17:4,8,17,20 19:9 19:11,13,15,18,23 20:20 21:16 22:1 22:13,22 24:3,9
W want 15:1,3 20:13 45:21,25 54:21 59:14 70:6 76:3 111:12 wanted 57:24 warrant 25:10 Washington 1:21 2:11 wasn't 25:21 59:25 73:6 92:20 93:1,6 waste 53:8 63:21 wasting 56:11,13 60:23 62:9 63:25 way 15:4 17:7,25 22:1,6 55:14 56:11 66:23 77:8 83:11 92:1 94:9 113:15 ways 17:5,14,16,20 17:23 weak 98:20 Wednesday 1:15 2:4 We'll 8:19 we're 9:1 70:24 84:9 86:6 105:18 we've 45:20 49:4 60:6 86:13 96:18 WHEREOF 113:17 wireless 7:7,17,25 22:25 23:18,20 36:9 92:20,25 93:11 96:22 witness 2:1 9:25 37:20 46:1 95:8 100:23 108:10	Y yeah 45:23 53:24 65:24 66:3 87:13 97:1 years 7:15 Yep 51:19 yesterday 12:11 Z zero 32:4,8,14 zeroed 25:11 1 1 35:3,7 41:5,8 46:8 46:11 47:16 48:12 79:14,16,18 80:20 98:11 103:12 1.1.0 80:12,25 1:00 112:17 10 4:5 65:22,23 98:11 10,425,817 1:8 4:5 4:6 100 46:3,4 1001 4:6 31:5,7	2 2 47:23 2G 37:3 71:5,6 2-bit 28:25 20 11:24 112:11 20004 1:21 2:11 2005 4:5 10:8,12 28:18 2006 4:4 6:21,23 101:1 202-389-5000 2:11 2025 1:14 2:5 113:19 21 52:7 214-978-4000 2:17 215 2:4 23 51:12,18 52:22 25 51:17 26 111:13,17 27 36:23	27 21:32 21:37:7 65:4 76:12,14,21 76:22 77:1,5,12 77:15 81:5,9 84:21 85:4,8 89:3 90:2,5,11,13,16 90:19 91:1,10,13 92:2 94:7,9,11 95:18 97:13,15 5.7.4.15 82:17,21 5.7.4.15.2-1 85:19 50 30:7 38:16 101:15 55 28:17,21 30:3 69:16 56 29:3 57 34:25 35:3,5,11 59 89:21,24 6 6 4:4 39:23 40:5,10 40:23 41:17,21,22 41:25 86:10,12,13 87:18 108:21,23 108:24,25 109:3 111:12,16,17 60 101:16 608 39:25 610 40:5 65 4:10 7 7 47:17 80:8,10 70 101:5 75201 2:16 8 8,005,219 4:9 8:58 1:15 2:5 80 101:6 817 9:5 12:22 13:1 13:3 14:24 15:11 15:20,25 16:4,5,7 16:10,12,16,25 17:4,8,17,20 19:9 19:11,13,15,18,23 20:20 21:16 22:1 22:13,22 24:3,9	

24:14,24 25:13,21
26:6 27:3,12,14
28:11,13 29:14,15
29:17,22,24 30:10
31:5 32:11 40:15
40:24 41:5 42:10
46:19 48:24 49:3
49:19 50:9,15
58:3,10,13,18
65:3 66:13,15,17
68:5,8,15 72:15
72:21 73:1,2,8,18
75:6 76:11 77:1,4
77:15,20,25 78:2
78:8,9,14,21
84:24 85:5,9 90:1
90:10 92:21 93:2
93:16 94:22 96:4

82 4:11

89 99:7

9

9 101:2,3,10,13

90 52:9

98 45:9,11,12