

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

CERTIFIED COPY

v.

WARD PARTICIPATIONS B.V.,

Patent Owner.

Case IPR2022-00113 (US Patent No. 10,992,480)

Case PGR2022-00007 (US Patent No. 10,992,480)

Case IPR2022-00114 (US Patent No. 11,063,766)

VIDEOCONFERENCE DEPOSITION OF

DR. BART PRENEEL

November 4, 2022

Page 1 - 70

8:13 a.m. EST - 10:39 a.m. EST

REPORTED BY:

Tamara L. Houston

CA CSR No. 7244, RPR, CCRR No. 140

Job Number 22-117175

Ref. 39843-0109IP1; 39843-0109PS1; 39843-0110IP1

THE SULLIVAN GROUP OF COURT REPORTERS

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

REMOTE VIDEOCONFERENCE DEPOSITION OF DR. BART
PRENEEL taken on behalf of the Petitioner, commencing
from 8:13 a.m. EST to 10:39 a.m. EST, Friday, November
4, 2022, before Tamara L. Houston, CSR No. 7244, CCRR,
RPR.

THE SULLIVAN GROUP OF COURT REPORTERS

1 APPEARANCE OF COUNSEL:

2

3 On behalf of the Petitioner:

4 FISH & RICHARDSON P.C.
5 BY: USMAN A. KHAN, PH.D., ESQ.
6 JEREMY MONALDO, ESQ.
7 1000 Maine Avenue SW
8 Suite 1000
9 Washington, DC 20024
10 (202) 626-6383
11 khan@fr.com
12 monaldo@fr.com

9 On behalf of the Patent Owner and Witness:

10 RAMEY LLP
11 BY: JACOB B. HENRY, ESQ.
12 5020 Montrose Boulevard
13 Suite 800
14 Houston, Texas 77006
15 (832) 454-1456
16 jhenry@rameyfirm.com

15 ALSO PRESENT: Scott Ward, Proprietor

16

17

18

19

20

21

22

23

24

25

THE SULLIVAN GROUP OF COURT REPORTERS

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

INDEX TO EXAMINATION

WITNESS: DR. BART PRENEEL

EXAMINATIONS	PAGE
Mr. Khan.....	6
Mr. Henry.....	62
Mr. Khan.....	64

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

None

THE SULLIVAN GROUP OF COURT REPORTERS

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

INDEX TO EXHIBITS

DR. BART PRENEEL

SAMSUNG ELECTRONICS CO., LTD. vs. WARD PARTICIPATIONS

B.V.

November 4, 2022

Tamara L. Houston, CSR No. 7244, CRR No. 140, RPR

EXHIBIT	DESCRIPTION	PAGE
	None.	
	--o0o--	

THE SULLIVAN GROUP OF COURT REPORTERS

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

Friday, November 4, 2022, 8:13 a.m. EST

--o0o--

Whereupon, DR. BART PRENEEL, having been called as a witness was duly sworn to tell the truth, the whole truth, and nothing but the truth testified as follows:

EXAMINATION BY MR. KHAN:

Q. Good afternoon, Dr. Preneel. I hope you're well.

A. Good morning.

Q. I wanted to first check with you and see if -- if you are in -- do you have -- have you taken any medication today or anything that would prevent you from speaking about your declaration?

A. No, I have not.

Q. Okay. Thank you.

So like the deposition earlier this week, I'll start off with some general questions before getting into more specifics. I'll provide you breaks periodically unless you specifically request them. Should you or Ms. Houston or anyone else here feel that we need to take a break, I'll request that you just give me a heads-up so I can wrap up the line of questioning.

Does that work for you?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. That's fine.

2 Q. And during the breaks, you understand that
3 you're not allowed to discuss the substance of your
4 testimony today with counsel of Ward?

5 A. I understand it.

6 Q. And would you agree to let me know if anyone
7 at any point communicates with you in any manner during
8 the course of the cross-examination regarding your
9 testimony today?

10 A. Yes, I will do that.

11 Q. Okay. Do you understand that you are being
12 deposed today for statements made in your declarations
13 submitted in support of Ward's two patent owner
14 responses in -- with respect to the '480 patent?

15 A. I do.

16 Q. And that the proceeding numbers are
17 PGR2022-0007, and IPR2022-00113?

18 A. Yes, they are.

19 Q. For purposes of our deposition today, when I
20 refer to "your declaration," I will be referring to the
21 declaration you submitted in the PGR proceedings, which
22 is PGR2022-0007 --

23 A. Okay.

24 Q. -- unless I specifically mention the other
25 declaration.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Does that sound okay to you?

2 A. That's fine.

3 Q. Great.

4 Do you agree that your testimony on both of
5 those declarations substantively overlaps?

6 A. Yes, I do.

7 Q. So if I ask you a question regarding your PGR
8 declaration, it would also apply to your IPR
9 declaration; is that correct?

10 A. That is correct.

11 Q. Thank you.

12 Do you understand that your testimony today is
13 sworn testimony taken under oath?

14 A. I understand that, yes.

15 Q. And do you understand that the oath you've
16 taken in this deposition today is as solemn as the oath
17 you would take if testifying at trial?

18 A. I understand that, yes.

19 Q. Do you understand that the deposition
20 testimony today can be used at a trial or subsequent
21 briefs in these proceedings?

22 A. Yes, I understand that.

23 Q. Did you review your declarations in the '480
24 patent in preparation for this deposition today?

25 A. Can you please clarify the question?

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Sure. Did you -- did you review your
2 declarations in the '480 patent in preparation for the
3 deposition today?

4 A. Yes, I did.

5 Q. And I know I asked you this in the beginning
6 of the call, but is there any reason why you would not
7 be able to speak to your declarations with full clarity
8 today?

9 A. No, there is not.

10 Q. In preparation for the deposition today, did
11 you confer with Ward's counsel?

12 A. We had a preparatory meeting on Monday, so
13 before the first deposition.

14 Q. Okay. And between the first deposition, which
15 was held on Tuesday for the '766 proceedings, and today,
16 have you been in communication with Ward's counsel?

17 A. No, I have not been in communication with
18 Ward's counsel in that period.

19 Q. Okay. So is it -- is it correct to say that
20 you -- is it -- is my understanding correct that you
21 were not provided any feedback on your testimony with
22 respect to the '766 deposition conducted earlier this
23 week from Ward's counsel?

24 A. No, I was not.

25 Q. Okay. Thank you.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Now, turning to the '480 declaration that you
2 submitted, did you write that declaration yourself?

3 A. Yes, I did.

4 Q. How long did it take you to write the
5 declaration?

6 A. I mean, I don't have recollection of the
7 details because this work was done almost a year ago,
8 but, of course, I spent a considerable amount of time
9 studying the patents and studying all of the documents
10 provided to me. So I think it was definitely an effort
11 of I think 10 to 15 working days, at least.

12 Q. I see.

13 A. And then I wrote -- of course, then the
14 writing of the text is -- just takes a few days --

15 Q. Did you draft all the parts yourself?

16 A. Of course, at the beginning, I think there is
17 some understanding of the applicable legal standards,
18 and yes, I was provided this. And of course, I went to
19 this and I made sure that I fully understood this.

20 Q. Okay. With respect to your '480 declarations,
21 are there any statements or remarks that you would like
22 to change?

23 A. No, there are not any.

24 Q. Now, to avoid -- well, as you know, the '766
25 and '480 have references that overlap and also share the

THE SULLIVAN GROUP OF COURT REPORTERS

1 same specification, so to avoid repeating many of the
2 questions and answers from our last session, I'll just
3 ask a few questions to confirm the applicability of some
4 of the questions that I asked earlier in the '766
5 deposition and how they may relate to today.

6 So in our last deposition on Tuesday
7 addressing the '766 declaration, do you agree that I
8 asked you questions on your background, such as your
9 experience?

10 A. Yes, I do.

11 Q. Are your answers to those questions the same
12 today with respect to the '480 declaration as they were
13 on Tuesday?

14 A. Yes, I confirm that those answers also apply
15 to the '480 declaration.

16 Q. We also discussed your views on the '766
17 patent, its disclosure such as the figures in -- such as
18 Figures 3 and Figures 4 on Tuesday.

19 Do you agree that your views on the disclosure
20 in the '766 patent also apply to the '480 patent?

21 A. There are, of course, differences between the
22 two patents, but where the patents are identical, of
23 course, my views are identical.

24 Q. Okay. And what are those differences between
25 the two patents?

1 A. Well, it's not so easy to answer that very
2 briefly, but I think there are differences. In
3 particular, when we look at Claims 17 and 18, where
4 there is a substantial difference in the sense that here
5 it is explained very clearly that a private key can also
6 be stored in a memory -- not necessarily in BIOS or a
7 secure memory -- and then this would be protected under
8 the keys securely stored, but this is a substantial
9 difference between the two patents.

10 And I think a second difference related
11 to protection of authentication software --

12 (Court reporter requested clarification.)

13 THE WITNESS: Second difference relates to the
14 protection of the authentication software.

15 And let me confirm that I have my note
16 correctly. In '480, the software is not necessarily
17 encrypted. It can be encrypted, but it is not
18 necessarily encrypted.

19 BY MR. KHAN:

20 Q. So when you say in '480 it is not necessarily
21 encrypted, are you saying that the -- the discussion of
22 the description of the encryption in '480 is different
23 than the one in the '766?

24 A. Yes, because in '480, it may be encrypted but
25 does not need to be encrypted.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. I'm sorry. Could you repeat that, please?
2 What was that?

3 A. In '480, it may be encrypted, but it does not
4 need to be encrypted.

5 Q. And that's because the '480 describes it
6 differently than the '766?

7 A. Yes, it does.

8 Q. So -- but with respect to our discussion,
9 would you agree that Figures 3 and Figures 4 of the '766
10 patent are the same as Figures 3 and Figure 4 of the
11 '480 patent?

12 A. Yes, they are.

13 Q. And to the extent that I had asked you
14 questions about Figures 3 and Figures 4 with respect to
15 the '766 patent, would you agree that your answers to
16 those questions also are applicable to the '480 patent?

17 A. It depends on a specific question, obviously.
18 I mean, a figure only makes abstractions and shows only
19 a high level view. If you go into the details, as I
20 mentioned in my previous answer, there may be subtle
21 differences.

22 Q. Okay. We'd also discussed your views on the
23 Ellison reference. Are your views on the Ellison
24 reference the same as they were on Tuesday?

25 A. Yes, they are.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Okay. If I could ask you to open up your
2 declaration, please, and turning to paragraph 26.

3 A. Yes.

4 Q. So like in your '766 declaration, you noted
5 that you used the BRI standard.

6 Did you use the same BRI standard to interpret
7 the '480 claims?

8 A. Yes, I did.

9 Q. Okay.

10 A. Could you confirm which paragraph this was?
11 Because I opened the '007 PGR document and
12 paragraph 26 --

13 Q. Yes. Paragraph 26 reads, "Patent claims in a
14 PGR are given their broadest reasonable interpretation
15 ('BRI')." "

16 Do you see that?

17 A. So we need the number of the document just to
18 be sure.

19 Q. So the -- it should be in link that I sent to
20 you --

21 A. Yes.

22 Q. All right. In that link, you should have seen
23 a file -- let's see. It should -- the filing should
24 be -- it should have your declaration.

25 A. Yes. The "Preneel '480 PGR Declaration."

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. That's right.

2 A. Yes.

3 Q. Yeah, so if you could open that file.

4 A. Yes, I did that.

5 Q. Great. And then paragraph 26 of that file.

6 A. 26 reads for me, "I have been part-time
7 advisor at Phillips Research."

8 Q. Okay. One second, please. Okay. I'm sorry.
9 It should be paragraph 37.

10 A. Okay. Thank you.

11 Q. I'm sorry.

12 So paragraph 37 states, "Patent claims in a
13 PGR are given their broadest reasonable interpretation
14 ('BRI')."

15 Is that correct?

16 A. That's correct.

17 Q. So is it correct that you used the BRI
18 standard to interpret the '480 claims?

19 A. Yes, I did.

20 Q. The last sentence on that same paragraph
21 reads, "The patent's entire disclosure, including the
22 specification and prosecution history, should be
23 considered to understand the BRI."

24 Is that correct?

25 A. That is correct.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. So just to clarify, the last three words --
2 the last phrase that ends that sentence, the "should be
3 considered to understand the BRI," did you mean to say
4 that the patent's entire disclosure, including the
5 specification and prosecution history, should be
6 interpreted under the BRI?

7 A. I can guess, I think, in the formulation for
8 me.

9 Q. Okay. All right. So it's correct to say that
10 in reviewing the '480 patent and the description of the
11 prosecution history and the claims, you -- you used the
12 broadest reasonable interpretation standard?

13 A. That is correct.

14 Q. Okay. Thank you.

15 Now, in the following paragraphs after that,
16 for example, in paragraphs 40 to 42 -- actually, 40 to
17 45, like in the '766 declaration, you discuss the legal
18 standards that you use; is that correct?

19 A. That is correct.

20 Q. Now, we had discussed on Tuesday your
21 understanding of the BRI standards like the IPR and PGR
22 obviousness and anticipation. Is that still the same?
23 Are your views and your understanding of these
24 concepts -- these legal concepts still the same as they
25 were on Tuesday for the '766?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. My views and understanding are still the same.

2 Q. Thank you.

3 I just want to get a better sense here. In
4 paragraph 41, you mention anticipation. And I wanted to
5 ask you if a combination of two references can
6 anticipate a claim.

7 A. I think it says so in the 42, "A claim can be
8 obvious when its elements are disclosed in two or more
9 references from the prior art, and there was a reason
10 for a person of ordinary skill to combine those
11 references to obtain the elements as claimed."

12 Q. So I'll just repeat the question.

13 A. Okay.

14 Q. Can a combination of two references anticipate
15 a claim?

16 A. So if -- I think I can only repeat the same
17 answer that, in fact, if two elements are disclosed in
18 two references from the prior art and there was a reason
19 for a POSITA to combine those references, then it can be
20 prior art.

21 Q. Okay. So if I can repeat the answer, my
22 understanding of your answer, when I asked you if
23 combination of two references can anticipate a claim,
24 you indicated that your answer is in paragraph 42, which
25 states that, "A claim can be obvious when its elements

1 are disclosed in two or more references from the prior
2 art."

3 Is that correct?

4 A. And there was a reason for a POSITA to combine
5 those references.

6 Q. Okay. Thank you.

7 So in paragraph 42, you mentioned that, "A
8 claim can be obvious," right, "when its elements are
9 disclosed in two or more references from the prior art."

10 Can a claim be obvious in a combination of
11 five or six references?

12 A. I think it can be, but the approach that we do
13 is -- I think it's the work step by step. And of
14 course, again, all the disclaimers have to apply. Also
15 for more than two, of course, so that the POSITA should
16 have a reason to obtain these elements of the claim.
17 It's not the existence of the references that is
18 sufficient.

19 Q. When you say "all of the disclaimers have to
20 apply," I'm not sure what you mean. Could you clarify,
21 please?

22 A. Well, because in your question you did not add
23 the phrase "and there was a reason for a person of
24 ordinary skill to combine those references."

25 Q. I see.

THE SULLIVAN GROUP OF COURT REPORTERS

1 In addition to what you said there, you quote
2 the language, "and there was a reason for a person of
3 ordinary skill in the art to combine those references."
4 When you look at two references, what are some of the
5 factors you consider when determining whether prior art
6 renders a claim obvious?

7 A. I think there has to be a natural way of
8 combining these things, so it's the case when you
9 combine things, I should not have to come up with a new
10 invention or new innovative step to actually achieve the
11 claim that would be obvious. So it should be actually
12 rather easy to take the two elements and to combine them
13 based on, I would say, standard expertise available to a
14 POSITA. I think that's an important element. The
15 combination should not by itself require an inventive
16 step.

17 Q. So when you are considering whether two
18 references can be combined, is it correct that your
19 conclusion would depend on whether there is some type of
20 inventive step involved in the combination of those two
21 references? Is that correct?

22 A. That is correct.

23 And I think a second element -- may I add,
24 which is the last sentence in paragraph 42, of course,
25 if you would in the combination render one of the

THE SULLIVAN GROUP OF COURT REPORTERS

1 references inoperable for its intended purpose, then of
2 course, you also don't have obviousness.

3 Q. Did you review the petition, the '480
4 petitions, the PGR and IPR petitions?

5 A. Yes, I did.

6 Q. And is it your understanding that both of
7 those petitions include obviousness grounds?

8 A. Yes. I understand that.

9 Q. And so did you also use the obviousness
10 standard to analyze the '480 patent?

11 A. Yes, I did.

12 Q. Okay. So in considering the -- like the
13 claims and the written description and the figures, you
14 considered the obviousness standard and then also
15 applied the same standard for the prior art; is that
16 correct?

17 A. Yes, that's correct.

18 Q. Thank you.

19 In the PGRs, there's a 112 ground, 35 USC 112
20 ground.

21 Are you familiar with what the 35 USC 112
22 ground is?

23 A. I'm afraid that I don't know the articles of
24 that all. I'm a technical expert, and I don't know the
25 details of a number. I guess I could review the

1 legislation and what I should use on these techniques,
2 but if you give me a number, I'm afraid I can't
3 reproduce the exact condition behind that.

4 Q. Yes. So in the PGR, there was a ground
5 indicating that the '480 claims did not have written
6 description.

7 Do you recall that?

8 A. I think I do. Yes.

9 Q. Now, are you aware that there is a statute
10 requiring a patent to provide a full written description
11 for its claims' subject matter?

12 A. Yes, I understand that. That's the purpose of
13 a patent is to, of course, give the description and then
14 give the claims, and indeed, the claims should be
15 substantiated by the description.

16 Q. And you understand that if it does not provide
17 the written description, then it can be found invalid;
18 is that correct?

19 A. Yes, I understand that.

20 Q. Thank you.

21 MR. KHAN: Can we take a two-minute break?

22 THE WITNESS: That's fine.

23 MR. KHAN: Great. Thank you.

24 (Recess: 8:41 a.m. to 8:47 a.m.)
25

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. So, Dr. Preneel, in the chat I shared another
3 file, if you don't mind downloading that.

4 A. I have downloaded the file.

5 Q. Great. Thank you.

6 So that is -- my apologies for the slight
7 confusion there. I think moving forward we'll use this
8 file. This is -- this is your PGR declaration. Your
9 previous file, so far we've discussed, had the same
10 contents, but I believe it was your earlier declaration.
11 So it had the same paragraphs just numbered differently.
12 It was from your earlier declaration. So --

13 A. Okay.

14 Q. Yeah, so I just -- you know, if you can open
15 that up, I'll confirm with you just that, for example,
16 the paragraphs we've been discussing -- this is
17 Exhibit 2012 -- the paragraphs we discussed were the
18 paragraphs related to the BRI standards, which you can
19 see in paragraph 26.

20 A. Yes, that's correct.

21 Q. Confirmed.

22 And we also discussed the anticipation and
23 obviousness standard that you can see here in
24 paragraphs 30 to 34.

25 Is that correct?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Yes, these are the same paragraphs.

2 Q. Great. Thank you. And my apologies there
3 again.

4 So turning to Exhibit 2012, in paragraph 46.
5 In paragraph 46, you state here that, "It is important
6 to point out that in cryptography private keys are
7 either bit strings, that is, finite sequences consisting
8 of binary zeroes and ones or algebraic objects."

9 Is that correct?

10 A. That is correct.

11 Q. Is it your position that that private keys can
12 only be bit strings or algebraic objects?

13 A. Well, they can always be represented as such.

14 Q. So just -- just the two of them? Just the
15 two, the bit strings or algebraic objects; is that
16 correct?

17 A. Well, you could choose -- if you invent the
18 private key or crypto system in which a private key is
19 words in a language, but you would still always be able
20 to represent those as bit strings, because you can
21 represent the characters as bit strings.

22 (Court reporter requested clarification.)

23 THE WITNESS: Yes. So you can -- you can --
24 you could invent a cryptographic system in which the
25 keys are words in a natural language, but you could

1 always represent those words character by character as
2 bit strings.

3 BY MR. KHAN:

4 Q. So you agree that a private key can only be a
5 bit string or an algebraic object?

6 A. I don't think that's what I said in my
7 previous answer. But I think in this comment in
8 cryptography, if you take the standard used algorithms,
9 which are in -- cryptographic standards are in
10 textbooks, they will have indeed keys consisting of
11 binary strings or algebraic objects which can be
12 represented by binary strings.

13 Q. So I suppose I'm trying to understand that.
14 When you said that the private keys -- so is it correct
15 in paragraph 46, you say, "Cryptography private keys are
16 either bit strings, that is, finite sequences consisting
17 of binary zeroes and ones or algebraic objects."

18 So my question --

19 A. I can represent that as finite number of bit
20 strings.

21 Q. Yes. Well, my question is very -- because you
22 used the word "either," I'm trying to understand that --
23 do you mean, then, that all cryptography private keys
24 can just be either bit strings or algebraic objects?

25 A. I think, indeed, that's what's the case in all

THE SULLIVAN GROUP OF COURT REPORTERS

1 crypto systems that are being used and that are being
2 described in textbooks.

3 Q. Is that the case for the disclosure in the
4 '480 patent as well?

5 A. Yes, it is.

6 Q. So any bit string in the '480 patent can --
7 sorry. On any private key in the '480 patent, in your
8 opinion, could only be a bit string or algebraic object;
9 is that correct?

10 A. Represented as a bit string, yes.

11 Q. So what are algebraic objects?

12 A. An algebraic object is an object described by
13 mathematics. This is typically --

14 (Court reporter requested clarification.)

15 THE WITNESS: -- an algebraic object such as a
16 group, a ring, or a field which has elements and
17 operations on those elements.

18 BY MR. KHAN:

19 Q. And what is a bit string?

20 A. A bit string is a finite sequence consisting
21 of binary zeroes and ones.

22 Q. Can a single bit be a bit string?

23 A. Yes, it is. It is finite and it consists of
24 zeroes and ones.

25 Q. Does it have to have any structure to it, or

THE SULLIVAN GROUP OF COURT REPORTERS

1 is it just a sequence of finite numbers? Zeroes and
2 ones?

3 A. Well, this is exactly why I have the
4 definition I give. So it's a finite sequence of zeroes
5 and ones or it's an algebraic object because that has
6 some structure into it.

7 Q. I was asking you about -- I'm sorry. I was
8 asking you about a bit string. In your -- what is a bit
9 string?

10 A. A bit string is a finite sequence of zeroes
11 and ones.

12 Q. Does it have structure?

13 A. Not necessarily but, of course, it can have
14 structure.

15 Q. Like what?

16 A. For some reason, you could decide to always
17 have two zeroes and two ones and two zeroes and two
18 ones, and you have a bit string with structure in
19 itself. Or you would have a bit string in which every
20 four consecutive bits amount to an integer between --

21 (Court reporter requested clarification.)

22 THE WITNESS: Or you can have a bit string in
23 which every consecutive sequence of four bits represents
24 an integer between zero and nine.

25 BY MR. KHAN:

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. So in this example you just gave, when -- I
2 guess by structure, you mean pattern, like you could
3 have the -- the sequence of bits could correlate to a
4 particular patent pattern -- is that --

5 A. For example, yes.

6 Q. Okay. So a bit string could be a sequence
7 of -- a finite sequence of zeroes and ones in --
8 according to some pattern or, in some cases, no pattern;
9 is that correct?

10 A. That's correct.

11 Q. And I guess, are there any other structural or
12 pattern requirements there; or is it just as long as you
13 have a finite sequence of binary zeroes and ones, you
14 have a bit string?

15 A. If you have -- if I have a sequence of binary
16 zeroes and ones, you have a bit string. Requirements on
17 the pattern would come from the cryptographic algorithm
18 for which it is intended, where it was a key.

19 Q. I see.

20 Can a computer have more than one bit string?

21 A. Yes.

22 Q. Are -- are all authentication tables bit
23 strings?

24 A. Yes, they can be represented as bit strings.

25 Q. My question was, are all authentication tables

1 bit strings?

2 A. All authentication tables can be represented
3 as bit strings.

4 Q. You say "can be." What do you mean by "can
5 be"?

6 A. Because you could also represent it in other
7 ways, potentially.

8 Q. So if -- if authentication tables can be
9 represented in other ways, then all authentication
10 tables are not bit strings; is that correct?

11 A. But if you write it in a computer, they will
12 end up being bit strings because that's how computers
13 represent objects. So if I have an authentication table
14 of any form or shape and I want to load it into a
15 computer, it will be there as a bit string. I will be
16 able to point to a bit string in the computer
17 corresponding to this authentication table.

18 Q. So you mentioned the authentication table may
19 have a form and a shape.

20 What type of form and shape do authentication
21 tables have?

22 A. That depends on the specific algorithm
23 selected. A natural way would be just a list of bit
24 strings where it has an index, an address running from,
25 say, 0 to 1 million, and for each entry you have a bit

THE SULLIVAN GROUP OF COURT REPORTERS

1 string of, say, like, 64 bits. But you could also
2 choose to have a table that again consists of a million
3 entries where each entry consists of six digits between
4 0 and 9.

5 Q. So --

6 A. They would represent those in the computer,
7 they would be again represented as bit strings, but with
8 a specific structure as we discussed before.

9 Q. Does an authentication table have rows and
10 columns?

11 A. It can be organized as a linear table with
12 rows, but it can also be organized as a matrix with rows
13 and columns.

14 Q. Does an authentication table have index to
15 specify a row and a column?

16 A. If the table consists of rows and columns, it
17 will have an index for the rows and an index for the
18 columns.

19 Q. What type of rows and columns does an
20 authentication table typically have?

21 A. I think that's a question which that's hard to
22 answer. It depends on the application. But typically,
23 like, I can give an example of an authentication table,
24 but there could be other applications or other context
25 where we have different tables. But one could have a

THE SULLIVAN GROUP OF COURT REPORTERS

1 table with, say, a thousand rows and a thousand columns,
2 and then there would be in this table a million values,
3 or bit strings, if you want to be in my definition.

4 (Court reporter requested clarification.)

5 BY MR. KHAN:

6 Q. Why are authentication tables used?

7 A. They can be used to authenticate a data item
8 or can be used to authenticate a person or a device.

9 Q. And what's the advantage of using an
10 authentication table versus a bit string?

11 A. Well, authentication table in the computer
12 would be represented as a set of bit strings. So in the
13 end, in that respect, there is not much difference.
14 It's just a different way of doing things. You can
15 authenticate data with a cryptographic algorithm. It
16 uses as key a bit string, or you could decide to
17 authenticate a data item using authentication table.
18 It's one way of -- another way -- there are different
19 ways of achieving the same goal.

20 Q. So if I may repeat your answer, you mentioned
21 that there's different ways to authenticate, and one way
22 is to use an authentication table, and another way is
23 using a bit string, and there are different ways of
24 performing the authentication; is that correct?

25 A. Well, they will be used in combination with a

THE SULLIVAN GROUP OF COURT REPORTERS

1 different authentication algorithm. And if you use a
2 table, you will have a bit more data to store, but you
3 may have fewer computations. If you use a short bit
4 string, you need obviously to store fewer data, but you
5 may have to do more computations.

6 Q. So the advantage of using a table,
7 authentication table, is that you will need to perform
8 fewer computations, and the disadvantage is that you
9 would have to store a bit more data; is that --

10 A. That's correct. Yes.

11 Q. And so is it fair to say that when you're
12 interested in performing a faster computation, you may
13 want to use a authentication table?

14 A. That is correct, yes.

15 Q. And you mentioned you might have to store a
16 bit more data; is that correct?

17 A. That's correct.

18 Q. What's that -- what's the additional data that
19 you typically store?

20 A. Well, you have to store authentication table
21 which consists of multiple bit strings.

22 (Court reporter requested clarification.)

23 BY MR. KHAN:

24 Q. And is it multiple bit strings because you
25 have different rows and columns?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. In each row and column element, you have to
2 store, indeed, a table element, and that's a bit string.

3 Q. So authentication table will have different
4 elements, and each element is a bit string; is that
5 correct?

6 A. That's correct, yes. Or it can be represented
7 as a bit string.

8 Q. And each element may have -- each element has
9 a row and column assigned to it that's part of the
10 authentication table; is that correct?

11 A. I would formulate it the other way around. I
12 would say to each row and column, you assign an element.

13 Q. Okay. And in order to do that, you would need
14 to also have information about the row number and the
15 column number; is that correct?

16 A. Can you clarify? In order to do what?

17 Q. So in order to store different elements or
18 different bit strings in an authentication table --

19 A. Yes.

20 Q. -- is it correct that you would then need a
21 mechanism to identify where in the table that particular
22 element or bit string is?

23 A. Yes. You have an index for the rows and an
24 index for the columns, and these are, again, bit
25 strings.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Is there a type of -- sorry. Are there bit
2 strings that are not authentication tables?

3 A. I think it's very hard to answer this question
4 because I could always, in principle, construct an
5 authentication table that corresponds to a certain bit
6 string if this bit string has sufficient length.

7 Q. I'll repeat my question because I'm not sure
8 you've answered the question.

9 My question was, are there bit strings that
10 are not authentication tables?

11 A. I think the answer is no because even a bit
12 string -- a single bit string is a table with one row
13 and one column and a corresponding authentication table
14 with one entry.

15 Q. Okay. So is -- I'm sorry. Can you still hear
16 me? My computer froze up a little bit. So just give me
17 a second.

18 A. I can hear you.

19 Q. Okay. Is a software identification number an
20 authentication table?

21 A. No, it's not an authentication table. An
22 authentication table is just --

23 (Court reporter requested clarification.)

24 THE WITNESS: Sorry. No, it is not an
25 authentication table. That was my answer. Apologies.

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. Going back to your declaration, paragraph 46.
3 At the end of 46, you state -- so you state that, "The
4 use of the terms authentication data and bit strings in
5 '480 can be deduced from the following examples."

6 Is that a correct reading of that sentence in
7 paragraph 46?

8 A. That is correct.

9 Q. And is it correct that in the following
10 examples that you mention, you point to three examples:
11 In column 4, lines 33 to 39; column 7, lines 45 to 48;
12 and column 10, lines 23 to 33 of the '480 patent?

13 A. That is correct.

14 Q. Is it correct that not a single one of these
15 quoted passages recites the words "authentication data"?

16 A. It is correct. Yes.

17 Q. To your knowledge, "authentication data" is
18 recited in other parts of the '480 patent; is that
19 correct?

20 A. That is correct.

21 Q. In paragraph 47 and I guess subparagraph g,
22 it's on page 19 of Exhibit 2012.

23 Do you see that?

24 A. Yes.

25 Q. And this -- here you're quoting column 9,

THE SULLIVAN GROUP OF COURT REPORTERS

1 lines 35 to 56 of the '480 patent; is that correct?

2 A. That is correct.

3 Q. Now, in this section, g, you have italicized
4 one sentence and bolded the following sentence. That
5 the sentence -- sorry.

6 You've italicized two sentences and bolded the
7 sentence that follows the italicized two sentences; is
8 that correct?

9 A. That is correct.

10 Q. Was there a reason why you italicized one and
11 bolded the others? I'm just trying to understand, you
12 know, what the difference was.

13 A. I think they're just key points of this
14 paragraph I wanted to draw the attention to.

15 Q. Now, in these key points, you mention a Ring 0
16 processing environment; is that correct?

17 A. That is correct.

18 Q. What is a Ring 0 processing environment?

19 A. That's a processing environment of a processor
20 with the highest privilege.

21 Q. When you say "highest privilege," can you
22 clarify what that means?

23 A. It means that this environment can access
24 information which higher rings -- Rings 1, 2, and 3 and
25 so on -- cannot access. So it's used to control the

1 processor and to organize the processor.

2 Q. So is it correct to say that Ring 0 has the
3 least level of access privileges?

4 A. I would prefer to rephrase that and say as the
5 highest level of access privileges in the sense that it
6 can do more, but of course, fewer entities have access
7 to this. So the user applications do not have access
8 typically to Ring 0.

9 Q. Now, you used the word "typically."
10 Does that mean that in some cases it can be
11 accessed by user-operated software applications?

12 A. I think it's real applications can request the
13 kernel running in Ring 0 to do certain things, but they
14 cannot see what is happening there. Why do I say
15 "typically"? Because people have conceived operating
16 systems where there is no separation between user and
17 kernels, so very simplified systems. And there have
18 been cases where there were flaws in the kernel software
19 giving the users this kind of access. But if a computer
20 is probably -- properly configured and operated, user
21 applications will not have access to the Ring 0.

22 Q. So is it fair to say, then, that in some
23 systems, user applications can have access? Those would
24 be the simpler systems. And in other systems, the user
25 applications are restricted from access at Ring 0; is

1 that correct?

2 A. I would rephrase this because, maybe to
3 clarify, when I speak of those simpler systems, those
4 are typically not systems with users. Those are systems
5 operating a washing machine or systems operating sensor
6 notes. But if we have user applications, which means we
7 have browsers and word processing tools, then they will
8 not have access to Ring 0.

9 Q. So your answer -- last answer mentioned the
10 word "typically" again. Just to clarify, I'm not asking
11 for the typical situations. I'm asking about what's
12 possible, right? And so when I ask you about user
13 applications, you know, I'm asking, is it possible that
14 some user applications have access to Ring 0 and in
15 other systems the user applications do not have access
16 to Ring 0? Is that correct?

17 A. If I give my answer for Windows machines,
18 macOS, and Linux machines, they have no access.

19 (Court reporter requested clarification.)

20 THE WITNESS: Windows machines, macOS, so
21 the -- like the Apple systems, and the Linux systems --
22 user applications will not have access to Ring 0.

23 BY MR. KHAN:

24 Q. So if you limit to Window machines or -- I'm
25 sorry, micro -- what was it? Micro?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. MacOS, operating system by Apple. And I think
2 also --

3 Q. I see. I see. Okay.

4 A. I should also add the mobile devices, Android
5 and iOS.

6 Q. And so when you say it has the highest level
7 of access privilege, Ring 0 -- is that correct?

8 A. That's correct.

9 Q. Is it correct to say that it also is the most
10 restricted level of -- of the rings in the sense that
11 whatever processing goes on in Ring 0 can be restricted
12 to the highest degree compared to the other Ring levels?

13 A. Yes, fewer processors have access to this.

14 Q. Turning to paragraph 54 of your declaration.
15 Please let me know when you're there.

16 A. Yes, I'm there.

17 Q. Is it correct that paragraph 54 states, "The
18 '480 patent does not provide the authentication
19 software" -- sorry -- sorry, scratch that.

20 It says, "The '480 patent does not provide
21 that the authentication software would have (undefined)
22 access to its own private key by requesting such access
23 from any other software component."

24 Is that correct?

25 A. That is correct, yes.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Can you clarify what you mean by "undefined"
2 here?

3 A. I think "undefined" means here in a not
4 previously specified way. And it could also -- so, for
5 example, it could be read access or write access, or
6 what is meant is any form of access.

7 Q. So is it -- is my understanding correct if I
8 interpret that as saying that the '480 patent does not
9 provide that the authentication software would have
10 predetermined access?

11 A. I would say any form of access.

12 Q. Any form of access.

13 So it would have any form of access, or it
14 would not have any form of access?

15 A. Does not provide that authentication software
16 would have any form of access to its own private key by
17 requesting such access from any other software
18 component.

19 Q. So what you're saying -- in paragraph 54,
20 you're saying, the '480 patent does not provide that the
21 authentication software would have any form of access to
22 its own private key by requesting such access from any
23 other software component; is that correct?

24 A. Yes.

25 Q. When would the authentication software request

1 access from another software component? Access to its
2 own private key?

3 A. One can imagine that this private key is under
4 control of another process and has to have access to
5 this. Imagine a very simple example where you would
6 work with a smart card, insert it in the computer. Then
7 authentication software would have to request access to
8 this smart card.

9 Q. In that example of the smart card, is the
10 private key the smart card's private key, or is the
11 private key the authentication software's private key?

12 A. It could be the key stored in the smart card,
13 and I guess given that we use the term "software
14 component," we should speak of virtual smart card. So
15 it could be the private key of the authentication
16 software but stored in some other piece of software,
17 such as a virtual smart card.

18 Q. So in that example that you're saying, the
19 authentication software's private key is stored
20 somewhere else, not with the authentication software,
21 and in that case, it would be requesting access to
22 whichever other storage or memory component that might
23 be storing that private key; is that correct?

24 A. That is correct.

25 MR. KHAN: We've been going a little bit over

THE SULLIVAN GROUP OF COURT REPORTERS

1 an hour, so if you'd like to take a break here, you
2 know, it might be a good time to take a break. Now
3 would you like maybe a ten-minute break?

4 THE WITNESS: Okay.

5 MR. KHAN: Great. Thank you.

6 (Recess: 9:27 a.m. to 9:37 a.m.)

7 MR. KHAN: I think at the beginning we didn't
8 note all of the attendees today. Do you want to make a
9 note of that now?

10 (Discussion off the record.)

11 MR. KHAN: Okay. Yeah. I think it will be
12 great to have it on the record.

13 So on the Petitioner's side, we have myself,
14 Usman Khan, and my colleague, Jeremy Monaldo.

15 And, Jacob, if you'd like to talk about the
16 patent owner's --

17 MR. HENRY: Sure. On the patent owner's side,
18 we have myself, Jacob Henry, we have Dr. Bart Preneel,
19 and observing is patent owner, Scott Ward.

20 MR. KHAN: Thank you.

21 MR. HENRY: You're welcome.

22 BY MR. KHAN:

23 Q. Great. So I'll continue.

24 So before the break, we were at paragraph 54
25 and I was asking for some clarification regarding the

THE SULLIVAN GROUP OF COURT REPORTERS

1 term "undefined."

2 I wanted to get a little bit more
3 clarification on some of the discussions in the
4 declaration. In paragraph 40 -- so in paragraph 46 and
5 in a few other places, you use the term "can be," right?
6 So, for example, in paragraph 46, the first sentence --
7 you talked about this earlier -- you'd mentioned, "The
8 finite sequences consisting of binary zeroes and ones or
9 algebraic objects (such as two prime numbers, finite
10 field elements) that can be represented as a finite
11 number of string bits [sic]."

12 Is that correct?

13 A. That's correct, yes.

14 Q. Okay. So you mentioned the word "can be" --
15 words "can be" in a few different places, and I wanted
16 to understand that when you say "can be," do you mean
17 it's possible? Or do you mean something else?

18 A. Well, in this case it means it's possible, but
19 of course, as I mentioned before, if you represent it in
20 a computer, then you will do it as a finite number of
21 bit strings.

22 (Court reporter requested clarification.)

23 THE WITNESS: But if you do a calculation on
24 paper, you could work with digits 0 to 9.

25

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. So when we say that -- as an example, when we
3 say "X can be Y," is it correct that, consistent with
4 your use of the word "can be," "X can be Y" would mean
5 that X can, in some cases, be Y and, in other cases,
6 does not have to be Y; is that correct?

7 A. I'm not sure this is the correct
8 interpretation here. And in any case, we would have to
9 do it for every occurrence. I'm happy to repeat the
10 clarification I gave.

11 So I think here "can be" means it is
12 technically possible to do this, and the additional
13 clarification provided is that this is the way that it
14 is done in computer systems.

15 Q. Okay. So maybe we can re- -- maybe we can
16 visit some of the other iterations of the phrase "can
17 be." In paragraph 55 -- please let me know when you're
18 there.

19 A. Yes, I'm there.

20 Q. Paragraph 55 states, "Because the private key
21 can be an integral part of the authentication software";
22 is that correct?

23 A. That is correct.

24 Q. So here, when you say "private key can be an
25 integral part of the authentication software," are you

THE SULLIVAN GROUP OF COURT REPORTERS

1 saying it's technically possible that the private key is
2 an integral part of an authentication software?

3 A. Yes, it is.

4 Q. And paragraph 55, you have no citation to that
5 statement you made; is that correct?

6 A. That is correct.

7 Q. So is it correct that the private key can also
8 not be an integral part of the authentication software?

9 A. That is correct.

10 Q. So when you make the statement "the private
11 key can be an integral part of the authentication
12 software," is that -- kind of when you're interpreting
13 the '480 patent in view of the obviousness standard,
14 you're saying, "Yeah, it would be obvious that the
15 private key can be an integral part of the
16 authentication software"; is that correct?

17 A. That is correct, yes.

18 Q. Turning to paragraph 67. Please let me know
19 when you're there.

20 A. Yes, I'm there.

21 Q. In paragraph 57 [sic], you state, "In the '480
22 patent, a private key can be authentication data."

23 Is that correct?

24 A. Yes.

25 Q. So consistent with your earlier statement,

THE SULLIVAN GROUP OF COURT REPORTERS

1 here when you say "a private key can be authentication
2 data," are you saying that it's technically possible for
3 a private key to be authentication data? Is that
4 correct?

5 A. That is correct.

6 Q. And consistent with the meaning of that term,
7 it's also possible that the private key cannot be
8 authentication data; is that correct?

9 A. That is correct.

10 Q. And so when you make the statement "a private
11 key can be authentication data," it's again because a
12 person of ordinary skill in the art would have found it
13 obvious in view of the '480 patent; is that correct?

14 A. That is correct.

15 Q. In paragraph 94, please let me know when
16 you're there.

17 A. Yes, I'm there.

18 Q. Paragraph 94, the last three words, the closed
19 parentheses that says, "Insert references here."

20 Is that correct?

21 A. That is correct.

22 Q. Was that a typo?

23 A. I think that was intended to be corrected, but
24 then due to time pressure, apparently this did not
25 happen. But I'm sure that counsel, if that would be

THE SULLIVAN GROUP OF COURT REPORTERS

1 allowed, can provide you with those references later on.

2 Q. So as the declaration was submitted, there's
3 no citation to any references in paragraph 94; is that
4 correct?

5 A. That is correct.

6 Q. Would you also agree that there is no citation
7 in the entire Section B of your declaration which
8 extends from paragraph 52 to 71?

9 A. I would have to clarify that.

10 Q. Please go ahead and take your time.

11 A. That is correct.

12 Q. Is it also correct that paragraphs 76 to 95 in
13 Section D of your declaration include no citations?

14 A. That is correct, but I want to point out that
15 they do refer to Ellison and Muir, the specific numbers
16 in the figures in those patents.

17 Q. You mean like the reference numbers in Ellison
18 and --

19 A. Yes.

20 Q. I see.

21 But there's no citations; is that correct?

22 A. No. That is correct.

23 Q. So is it fair to say that from paragraphs 52
24 to 71 and 76 to 95, you describe the references and make
25 technical points without a single citation?

1 A. That is correct, yes. But these things -- but
2 these statements are -- in having obtained as a
3 consequence of careful study of the references,
4 including the patents.

5 Q. What is an encryption key?

6 A. Can you refer to a specific clause in this
7 document, or is there a figure in the patent you want me
8 to refer to?

9 Q. No. Just generally, what's your understanding
10 of what an encryption key is?

11 A. An encryption key is a key used in a
12 cryptographic algorithm.

13 Q. How is it used?

14 A. Can be used to encrypt data but can also be
15 sometimes used to decrypt data because the key for
16 encryption and decryption can be the same. An
17 encryption key can also be used to authenticate data or
18 to verify authentication of data, and obviously an
19 encryption key can also be used to encrypt or decrypt
20 another key.

21 Q. So if an encryption key is not used to perform
22 encryption, is it still an encryption key?

23 A. An encryption key can be used for multiple
24 purposes, and sometimes the same key is used for
25 multiple purposes and it will still be called an

1 "encryption key."

2 Q. So I'll repeat my question because I don't
3 think it was fully answered.

4 My question was, if an encryption key does not
5 perform encryption, can it still be called an encryption
6 key?

7 A. My statement would here be that if you write a
8 scientific paper, you would probably use a specific term
9 for this and you would not do this. I have seen in
10 patents sometimes that encryption key is used as a more
11 general term for a cryptographic key. So a key used for
12 any algorithm, also another algorithm for encryption and
13 decryption.

14 Q. So in the context of the '480 patent, when you
15 see an encryption key -- for example, encryption key 46
16 in Figure 3 --

17 A. Yes.

18 Q. -- is that a -- just a general cryptographic
19 key, or is it performing encryption and decryption or
20 both?

21 A. I think to answer that exactly, I would have
22 to go through all of the uses in the description of the
23 patent, but the first purpose is indeed encryption and
24 decryption of data or a key. But it could be that you
25 can actually authenticate data by encrypting it, and

THE SULLIVAN GROUP OF COURT REPORTERS

1 then the operation done with an encryption key is an
2 authentication.

3 (Court reporter requested clarification.)

4 THE WITNESS: To use an encryption key to --
5 sorry. I'm not sure I can rephrase it exactly the same.

6 But one could use an encryption key to
7 authenticate data as well. An encryption key can be
8 used to encrypt data as a form of authentication. Maybe
9 that's a better way of expressing it.

10 BY MR. KHAN:

11 Q. So if a key performs authentication but does
12 not perform encryption, are you saying that that key can
13 still be called an encryption key?

14 A. I think that would be possible, yes. It would
15 not be my preferred terminology, but I think it would be
16 possible.

17 Q. So in your opinion, an encryption key -- I'm
18 sorry. In your opinion, a key can be an encryption key
19 even though it does not perform encryption?

20 A. Yes, that would be possible.

21 Q. And so if there is a authentication key that
22 performs no encryption or decryption, it could be called
23 an encryption key; is that correct?

24 A. I think that would be possible. Again, it
25 would not be my preferred way of denoting it, but it

THE SULLIVAN GROUP OF COURT REPORTERS

1 could be understood like this, yes.

2 Q. Why would it not be your preferred way?

3 A. Because it's easier to clearly indicate what
4 the purpose of a key is, and it is in general better to
5 use a key only for one purpose. But there are
6 applications where these rules are not followed.

7 Q. Does the '480 patent follow those rules or
8 does not follow those rules?

9 A. I would have to double-check this, but I don't
10 think it follows those rules completely.

11 Q. And what makes you think that?

12 A. I think I would have to go to detailed
13 references to point out where these keys are being used
14 in which way.

15 Q. Okay. If you'd like to take the time to do
16 that, we can -- we can do that.

17 A. You want me to find all of the occurrences, or
18 would it be okay if I find just one of them?

19 Q. Yeah, I think one of them is fine.

20 A. So in Patent '480, column 5, lines 39 to 43,
21 "The authentication software preferably has its own
22 unique serial number, software ID and/or private
23 encryption key."

24 Q. So does that -- and this is column 5, lines 39
25 to 40; is that correct?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. That's correct.

2 Q. Does it tell you there whether it uses that
3 private encryption key for encryption or other purposes?

4 A. Well, it leaves it open, but the software
5 could use this key also for authentication.

6 Q. I see. And so this is because a person of
7 ordinary skill in the art looking at this description
8 would have found it obvious in view of what a private
9 encryption key is; is that correct?

10 A. That's correct. Yes.

11 Q. So can an encryption key be a public
12 encryption key, or can it also be a private encryption
13 key?

14 A. An encryption key can be a public encryption
15 key, but then we use a different form of cryptography
16 called asymmetric encryption where we have a different
17 key for encryption and decryption. And in that case,
18 the encryption key can be public but the decryption key
19 is always secret.

20 But if we have symmetric cryptography, then we
21 use the same key for encryption or decryption, or at
22 least a decryption key can be derived easily from the
23 encryption key. And in that case, of course, it cannot
24 be made public because that would defeat the purpose of
25 having encryption.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. So if I understood you correctly, you're
2 saying that when we use symmetric encryption, an
3 encryption key cannot be a public encryption key. When
4 we use asymmetric encryption, then we can have a public
5 key and some other form of a public key; is that
6 correct?

7 A. When we use asymmetric encryption, we have a
8 public key for encryption and a private key for
9 decryption.

10 Q. Right. Okay. And is the encryption key used
11 to encrypt any kind of data?

12 A. An encryption key can be used to encrypt data
13 or keys, yes.

14 Q. So -- I see.

15 So an encryption key can be used to encrypt a
16 private key?

17 A. That's correct.

18 Q. So when we say an encrypted private key,
19 that's a private key that has been encrypted; is that
20 correct?

21 A. That is correct.

22 Q. And when we say a private encryption key, that
23 is a key that is private that is used to perform
24 encryption; is that correct?

25 A. I think we've been there before. So private

1 means you don't make it public. But as I explained, the
2 term "encryption key" can also -- is also sometimes used
3 for other cryptographic algorithms such as
4 authentication algorithms.

5 (Court reporter requested clarification.)

6 BY MR. KHAN:

7 Q. The encrypted private key -- is an encrypted
8 private key a -- essentially a private key that has had
9 some form of encryption performed on it? Is that
10 correct?

11 A. That is correct.

12 Q. But a private encryption key does not have to
13 have had any encryption performed on it yet; is that
14 correct?

15 A. The term "private encryption key," here
16 private means that it should be protected, so it should
17 remain confidential or private. So it has to be
18 protected either by encrypting it or by storing it in a
19 memory that is not accessible to unauthorized parties.

20 Q. Sorry. Private encryption key can be one that
21 is stored in a protected location?

22 A. That is correct, yes.

23 Q. Do you agree that the term "private key" is
24 recited in the '480 claims?

25 And we can just look at --

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I have the -- yes, the term "private key" is
2 used in this area. Yes, of course.

3 Q. Do you agree that the term "private key" is
4 recited in the '480 patent in the paragraph beginning on
5 column 13, line 31?

6 A. Yes, that is correct.

7 Q. And what does this paragraph say that the
8 private key can be?

9 A. I will read the paragraph. "In a further
10 embodiment, the authentication software may be provided
11 with a system for signing a digital signature according
12 to the present invention using at least a part of a
13 software authentication number (software ID) or any
14 other application identifying character string,
15 hereinafter referred to as a private key."

16 So could you please repeat your question so
17 I'm sure that I answer it correctly?

18 Q. My question was, how does this paragraph
19 describe what a private key is?

20 A. This says that part of a software
21 identification number or any character string that
22 identifies an application can be used as a private key.

23 Q. Is a software ID number an encryption key?

24 A. A software ID number is a bit string and can
25 be used as an encryption or authentication key. I think

1 here specifically it will be used for signing a digital
2 signature, so it will be used for authentication. But
3 as we discussed before, for such kind of key, sometimes
4 the generic term "encryption key" is used.

5 Q. So I heard you say that the software ID can be
6 an encryption key again. But I was asking you, to be
7 more clear, does the '480 patent teach that the software
8 ID number can be an encryption key?

9 A. What this paragraph teaches is that at least
10 part of a software ID number, in this case it's an
11 encryption key for assigning a digital signature.

12 Q. Can you tell me where in that paragraph it
13 says "encryption key"?

14 A. It doesn't use this term, but as we discussed
15 before, the term "encryption key" is used in the broader
16 sense in these patents --

17 Q. Okay. So --

18 A. -- and the cryptographic key.

19 Q. So you're saying that even though this
20 paragraph doesn't describe an encryption key, it would
21 have been obvious that the private key is the encryption
22 key; is that correct?

23 A. If people would refer to this key as an
24 encryption key, I would understand what is meant by it,
25 yes.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. I'm sorry. Can you repeat that, please?

2 A. If someone would refer to this private key as
3 an encryption key, I would refer -- I would understand
4 what is meant by it, yes.

5 Q. I guess I can ask you. I've wanted to ask if
6 someone said it. I was asking if the '480 patent says
7 it.

8 So do you know if the '480 patent says that
9 the software ID number can be an encryption key?

10 A. In this paragraph, it doesn't say this.

11 Q. But --

12 A. But I think --

13 Q. Sorry. Go ahead.

14 A. But I think in the paragraph we discussed
15 before, that the term "encryption key" was used in a
16 broader sense.

17 Q. Which -- that was the paragraph describing the
18 authentication software; is that correct?

19 A. That's correct, yes.

20 Q. And that was in column 5, lines 39 to 40; is
21 that correct?

22 A. That's correct.

23 Q. So you're saying that someone looking at
24 column 5, lines 39 to 40, and someone looking at
25 column 13, lines 31 to, say, 56 or so would have

THE SULLIVAN GROUP OF COURT REPORTERS

1 understood that a software ID can be a private -- can be
2 an encryption key; is that correct?

3 A. That's correct, yes.

4 Q. And that's because it would have been obvious
5 to a person of ordinary skill in the art reading those
6 two passages; is that correct?

7 A. Yes.

8 Q. Okay. Even though it does not -- the '480
9 patent does not explicitly say so; is that correct?

10 A. That's correct.

11 Q. That same paragraph in column 13, lines 31
12 onwards, that starts off with the phrase "in a further
13 embodiment"; is that correct?

14 A. Yes, that's right.

15 Q. What does embodiment mean to you?

16 A. It means a specific realization of the system
17 described in the patent or matter described in the
18 patent with some of the elements specified.

19 Q. So in this paragraph when they say "in a
20 further embodiment," what's your understanding of what
21 they mean by "further embodiment"?

22 A. It means that you specify more details.

23 Q. Is it the case that patents can have multiple
24 embodiments, or do they have to have a single
25 embodiment, like a single invention, single embodiment?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Patents can have multiple embodiments.

2 Q. Does -- is it your understanding that
3 basically what we're seeing here in column 13, line 31
4 onwards, it's just another embodiment that is described
5 by the '480 patent? Is that right?

6 A. That's correct. Yes.

7 Q. And that when you look at this embodiment and
8 combine it with the other embodiments that are disclosed
9 in the '480 patent, that it would have been then obvious
10 that it discloses a private key in the manner that's
11 claimed; is that correct?

12 A. That's correct.

13 Q. And is that how you also arrived at your
14 statement in your declaration in paragraph 53?

15 A. Let me go back to that statement. Yes,
16 indeed.

17 Q. Then going back to the column 13, line 31
18 onwards, that particular passage discloses that the
19 second transaction party only stores the signed digital
20 signature and that the private key is generated by a
21 third party and sent to the second party for storage; is
22 that correct?

23 A. That's correct.

24 Q. This passage does not describe a second party
25 as providing the private key; is that correct?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I will have to read the full paragraph in
2 detail before I can confirm that.

3 Q. I'm sorry. I should have given you time to
4 read it first, so please take your time to read it.

5 A. Okay. Can you now please repeat your
6 question?

7 Q. Yes. My question is that -- actually, I'll
8 restart my line of questioning.

9 So do you agree that this passage discloses
10 the second transaction party as only storing the signed
11 digital signature and that the private key is generated
12 by a third party and sent to the second party for
13 storage?

14 A. That is correct. Yes.

15 Q. This passage does not describe the second
16 party as providing the private key; is that correct?

17 A. That is correct.

18 Q. The private key is provided by the third
19 party; is that correct?

20 A. That is correct.

21 Q. When the third party is providing the private
22 key and the transaction is between the first transaction
23 party and the second transaction party, would the third
24 transaction party provide the private key to both the
25 first transaction party and the second transaction

1 party?

2 A. No, it would not. What is described here can
3 be summarized as outsourcing the verification of the
4 digital signature to a TTP.

5 (Court reporter requested clarification.)

6 THE WITNESS: Outsource. Digital signature
7 verification to a trusted third party.

8 BY MR. KHAN:

9 Q. Could you please explain why it wouldn't
10 provide the private key to both the first transaction
11 party and the second transaction party?

12 A. I think the model described here is different.
13 So in order to reduce the cost and the efforts of the
14 second party in the transaction -- that could be, say,
15 the merchant who sells good -- rather than having the
16 merchants buy and operate infrastructure to store keys
17 and verify transactions, the merchant will only store
18 the signature with the transaction and then ask the
19 third party later in case of dispute to perform the
20 verification. And because the second party does not do
21 the verification, it does not need the keys.

22 Q. Okay. So it -- it just -- so the second
23 transaction party here just stores the digital signature
24 but never has any access to the private key; is that
25 correct?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. That is correct.

2 Q. Okay.

3 MR. KHAN: Can we take a ten-minute break,
4 please?

5 (Recess: 10:18 a.m. to 10:26 a.m.)

6 BY MR. KHAN:

7 Q. So returning to the declaration, Section B
8 on -- starting on page 22 of your declaration, that's
9 entitled, "The Disclosure of the '480 Patent to One of
10 Ordinary Skill in the Art"; is that correct?

11 A. That is correct.

12 Q. And in paragraph 52, you note that, "Each
13 limitation is fully supported by the written description
14 of the '480 patent and that one of ordinary skill in the
15 art would readily recognize that the claim limitations
16 are based on the disclosure of the '480 patent."

17 Is that correct?

18 A. That is correct.

19 Q. And they would readily recognize the claim
20 limitations based on the disclosure of the '480 patent
21 in view of the obviousness standard that you've applied
22 consistently in reading the prior art and the '480
23 patent; is that correct?

24 A. That is correct.

25 Q. In paragraph 65, you refer to, "The '480

THE SULLIVAN GROUP OF COURT REPORTERS

1 patent describes the claim features of Claim 2"; is that
2 correct?

3 A. Yes, I do.

4 Q. Is there a discussion in your declaration as
5 to Claims 4 and 5 of the '480 patent?

6 A. No, there was not, I think, but I believe the
7 patent is clear in this respect.

8 (Court reporter requested clarification.)

9 THE WITNESS: Clear in this respect. Easy to
10 understand in this respect.

11 MR. KHAN: Thank you. No further questions
12 from me.

13 Jacob, would you like to redirect?

14 MR. HENRY: Yes, I just have a couple of
15 questions, Dr. Preneel.

16 THE WITNESS: Okay.

17 EXAMINATION BY MR. HENRY:

18 Q. Earlier there was a discussion of bit strings
19 and authentication tables. Do you remember that you
20 were asked about those terms?

21 A. Yes, I do remember that.

22 Q. Okay. Did you mean to say that all bit
23 strings correspond to authentication tables?

24 A. I think that's not really what I wanted to
25 say. I think authentication table -- an authentication

1 table can be mapped to a bit string. Okay? And, of
2 course, in a specific context where application tables
3 are used, there is a one-to-one mapping between
4 authentication tables and bit strings or every bit
5 string corresponds to an authentication table and every
6 authentication table corresponds to a bit string.

7 Q. But more generally in computing, bit strings
8 are used and exist but do not correspond to
9 authentication tables, correct?

10 A. That is correct. For example, if I have the
11 key of an encryption algorithm, then that's a 158-bit,
12 192-bit, or 256-bit string that does not correspond to
13 an authentication table.

14 Q. Earlier this morning you were asked about the
15 difference between the '480 patent and the '766 patent.
16 And the word "describes" was bandied about.

17 Do you remember that?

18 A. Yes, I do remember.

19 Q. The difference between the two patents lies in
20 what they claim; is that not true?

21 A. That is correct.

22 MR. HENRY: Okay. I pass the witness.

23 MR. KHAN: Thank you. I have a few follow-up
24 questions.

25 MR. HENRY: Did you say "no follow-up

1 questions"?

2 MR. KHAN: No. I said I have a few follow-up
3 questions. Thank you.

4 FURTHER EXAMINATION BY MR. KHAN:

5 Q. So, Dr. Preneel, I just would like to get some
6 clarification. We talked about bitstreams [sic] and
7 authentication tables just now. And I think there's a
8 little bit of confusion because of the words "can be,"
9 right? Maybe we can speak about it in the context of
10 the '480 patent specifically.

11 In the '480 patent, are the authentication
12 table -- are all the -- are the bit strings
13 authentication tables?

14 A. Some bit strings are and some are not. One
15 can implement the '480 patent where it's symmetric
16 traditional cryptography as well and using -- for
17 example, for encrypting a key or also for generating a
18 digital signature, one can just use a bit string that
19 does not correspond to an authentication table.

20 Q. Now, we had earlier talked about some
21 advantages and disadvantages of using authentication
22 tables and bitstreams. And you had mentioned that it's
23 advantageous to use an authentication table perhaps when
24 you need to perform fewer computations; is that correct?

25 A. That is correct.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Is that also the case for the '480 patent?

2 A. That is correct, but that does not mean that
3 one has to use everywhere authentication tables.

4 Q. So some places where '480 patent talks about a
5 bit string, it could be authentication table, and other
6 places it may not be authentication table; is that
7 correct?

8 A. That is correct.

9 Q. And vice versa. In some places where it says
10 "authentication table," it could be a bitstream or it
11 could be something else?

12 A. Every authentication table will be represented
13 in a computer system by a bit string.

14 Q. Did you say "bit string" --

15 A. I said that before.

16 Q. -- or a "bitstream"?

17 A. "String." I think we've been using -- maybe I
18 misheard. But it's indeed not the word "stream." It's
19 "string." We've been discussing "bit string"
20 definition.

21 Q. And the authentication table in the '480
22 patent would also have rows and columns; is that
23 correct?

24 A. It would have rows and columns, but one could
25 have a case, as I -- we discussed before, there's only

THE SULLIVAN GROUP OF COURT REPORTERS

1 one row and one column.

2 Q. And to identify the rows and columns, it --
3 typically it would use an index system to identify which
4 row, which column; is that correct?

5 A. Yes. One would have a bit string indicating
6 the row and a bit string indicating the column.

7 Q. So in an authentication table in the '480
8 patent, you'd have the bit string indicating the row and
9 the column, a bit string which is the element within the
10 table as well; is that correct?

11 A. That's correct. All the -- both the integers
12 and the table values would be bit strings.

13 MR. KHAN: Great. No further questions.

14 MR. HENRY: I have no further questions.

15 COURT REPORTER: Counsel, may I get transcript
16 requests on the record, please.

17 MR. KHAN: Yes, please. If we could get a
18 rough draft today, that would be great.

19 COURT REPORTER: Of course.

20 MR. KHAN: Thank you.

21 COURT REPORTER: Mr. Henry, would you like a
22 rough --

23 MR. HENRY: Yes. Yes, please.

24 COURT REPORTER: Would you like a rough as
25 well?

THE SULLIVAN GROUP OF COURT REPORTERS

1 MR. HENRY: If it's not too much trouble.

2 COURT REPORTER: Not at all.

3 MR. HENRY: Okay. That sounds great, then.

4 Thank you.

5 (Whereupon the proceedings concluded at
6 10:39 a.m.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

THE SULLIVAN GROUP OF COURT REPORTERS

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

ERRATA SHEET

NAME OF CASE: SAMSUNG ELECTRONICS CO., LTD. V. WARD PARTICIPATIONS B.V.

DATE OF DEPOSITION: NOVEMBER 4, 2022

NAME OF WITNESS: DR. BART PRENEEL

Reason Codes:

1: To clarify the record.

2: To conform to the facts.

3: To correct transcription error.

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

DR. BART PRENEEL

DATED

THE SULLIVAN GROUP OF COURT REPORTERS

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

DECLARATION UNDER PENALTY OF PERJURY

I, DR. BART PRENEEL, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on November 4, 2022; that I have made such corrections as appear noted on the Deposition Errata Page(s), attached hereto, signed by me; that my testimony as contained herein, as corrected, is true and correct.

This Declaration is executed this _____ day of _____, 20____, at _____, California.

DR. BART PRENEEL

THE SULLIVAN GROUP OF COURT REPORTERS

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

)
STATE OF CALIFORNIA) ss.
)

I, Tamara Houston, RPR, CCRR, CSR No. 7244, a Certified Shorthand Reporter in the State of California, duly empowered to administer oaths, do hereby certify:

That, prior to being examined, the witness named in the foregoing deposition was by me duly sworn to testify to the truth, the whole truth, and nothing but the truth;

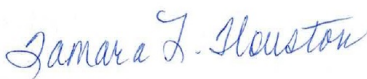
That said deposition was taken down by me in shorthand at the time and place therein named, and thereafter reduced to typewriting by computer-aided transcription under my direction;

That the dismantling, unsealing, or unbinding of the original transcript will render the reporter's certification null and void.

I further certify that I am not interested in the event of the action.

In witness whereof, I have hereunto subscribed my name.

Dated: November 8, 2022



TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

THE SULLIVAN GROUP OF COURT REPORTERS

Index: 'BRI'..9:37

<p>'</p> <hr/> <p>'BRI' 14:15 15:14</p> <hr/> <p>-</p> <p>--o0o-- 6:2</p> <hr/> <p>0</p> <p>0 28:25 29:4 35:15,18 36:2,8,13,21,25 37:8, 14,16,22 38:7,11 42:24</p> <p>007 14:11</p> <hr/> <p>1</p> <p>1 28:25 35:24</p> <p>10 10:11 34:12</p> <p>10:18 61:5</p> <p>10:26 61:5</p> <p>10:39 67:6</p> <p>112 20:19,21</p> <p>13 54:5 56:25 57:11 58:3, 17</p> <p>15 10:11</p> <p>158-bit 63:11</p> <p>17 12:3</p> <p>18 12:3</p> <p>19 34:22</p>	<p>192-bit 63:12</p> <hr/> <p>2 35:24 62:1</p> <p>2 35:24 62:1</p> <p>2012 22:17 23:4 34:22</p> <p>2022 6:1</p> <p>22 61:8</p> <p>23 34:12</p> <p>256-bit 63:12</p> <p>26 14:2,12,13 15:5,6 22:19</p> <hr/> <p>3 11:18 13:9,10,14 35:24 48:16</p> <p>30 22:24</p> <p>31 54:5 56:25 57:11 58:3, 17</p> <p>33 34:11,12</p> <p>34 22:24</p> <p>35 20:19,21 35:1</p> <p>37 15:9,12</p> <p>39 34:11 50:20,24 56:20, 24</p> <hr/> <p>4 6:1 11:18 13:9,10,14 34:11 62:5</p>	<p>40 16:16 42:4 50:25 56:20, 24</p> <p>41 17:4</p> <p>42 16:16 17:7,24 18:7 19:24</p> <p>43 50:20</p> <p>45 16:17 34:11</p> <p>46 23:4,5 24:15 34:2,3,7 42:4,6 48:15</p> <p>47 34:21</p> <p>48 34:11</p> <p>480 7:14 8:23 9:2 10:1,20, 25 11:12,15,20 12:16, 20,22,24 13:3,5,11,16 14:7,25 15:18 16:10 20:3,10 21:5 25:4,6,7 34:5,12,18 35:1 38:18, 20 39:8,20 44:13,21 45:13 48:14 50:7,20 53:24 54:4 55:7 56:6,8 57:8 58:5,9 61:9,14,16, 20,22,25 62:5 63:15 64:10,11,15 65:1,4,21 66:7</p> <hr/> <p>5 50:20,24 56:20,24 62:5</p> <p>52 46:8,23 61:12</p> <p>53 58:14</p> <p>54 38:14,17 39:19 41:24</p> <p>55 43:17,20 44:4</p> <p>56 35:1 56:25</p>	<p>57 44:21</p> <hr/> <p>6</p> <p>64 29:1</p> <p>65 61:25</p> <p>67 44:18</p> <hr/> <p>7</p> <p>7 34:11</p> <p>71 46:8,24</p> <p>76 46:12,24</p> <p>766 9:15,22 10:24 11:4,7, 16,20 12:23 13:6,9,15 14:4 16:17,25 63:15</p> <hr/> <p>8</p> <p>8:13 6:1</p> <p>8:41 21:24</p> <p>8:47 21:24</p> <hr/> <p>9 29:4 34:25 42:24</p> <p>94 45:15,18 46:3</p> <p>95 46:12,24</p> <p>9:27 41:6</p> <p>9:37 41:6</p>
--	--	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: a.m...bitstreams

A	24:4 46:6 53:23 54:3 59:9	applied 20:15 61:21	avoid 10:24 11:1
a.m. 6:1 21:24 41:6 61:5 67:6	ahead 46:10 56:13	apply 8:8 11:14,20 18:14,20	aware 21:9
abstractions 13:18	algebraic 23:8,12,15 24:5,11,17, 24 25:8,11,12,15 26:5 42:9	approach 18:12	B
access 35:23,25 36:3,5,6,7,19, 21,23,25 37:8,14,15,18, 22 38:7,13,22 39:5,6, 10,11,12,13,14,16,17, 21,22 40:1,4,7,21 60:24	algorithm 27:17 28:22 30:15 31:1 47:12 48:12 63:11	area 54:2	back 34:2 58:15,17
accessed 36:11	algorithms 24:8 53:3,4	arrived 58:13	background 11:8
accessible 53:19	allowed 7:3 46:1	art 17:9,18,20 18:2,9 19:3, 5 20:15 45:12 51:7 57:5 61:10,15,22	banded 63:16
achieve 19:10	amount 10:8 26:20	articles 20:23	Bart 6:3 41:18
achieving 30:19	analyze 20:10	assign 32:12	based 19:13 61:16,20
add 18:22 19:23 38:4	and/or 50:22	assigned 32:9	basically 58:3
addition 19:1	Android 38:4	assigning 55:11	beginning 9:5 10:16 41:7 54:4
additional 31:18 43:12	answers 11:2,11,14 13:15	asymmetric 51:16 52:4,7	binary 23:8 24:11,12,17 25:21 27:13,15 42:8
address 28:24	anticipate 17:6,14,23	attendees 41:8	BIOS 12:6
addressing 11:7	anticipation 16:22 17:4 22:22	attention 35:14	bit 23:7,12,15,20,21 24:2, 5,16,19,24 25:6,8,10, 19,20,22 26:8,10,18,19, 22 27:6,14,16,20,22,24 28:1,3,10,12,15,16,23, 25 29:7 30:3,10,12,16, 23 31:2,3,9,16,21,24 32:2,4,7,18,22,24 33:1, 5,6,9,11,12,16 34:4 40:25 42:2,21 54:24 62:18,22 63:1,4,6,7 64:8,12,14,18 65:5,13, 14,19 66:5,6,8,9,12
advantage 30:9 31:6	apologies 22:6 23:2 33:25	authenticate 30:7,8,15,17,21 47:17 48:25 49:7	bits 26:20,23 27:3 29:1 42:11
advantageous 64:23	apparently 45:24	authentication 12:11,14 27:22,25 28:2, 8,9,13,17,18,20 29:9, 14,20,23 30:6,10,11,17, 22,24 31:1,7,13,20 32:3,10,18 33:2,5,10, 13,20,21,22,25 34:4,15, 17 38:18,21 39:9,15,21, 25 40:7,11,15,19,20 43:21,25 44:2,8,11,16, 22 45:1,3,8,11 47:18 49:2,8,11,21 50:21 51:5 53:4 54:10,13,25 55:2 56:18 62:19,23,25 63:4, 5,6,9,13 64:7,11,13,19, 21,23 65:3,5,6,10,12,21 66:7	bitstream 65:10,16
advantages 64:21	Apple 37:21 38:1		bitstreams 64:6,22
advisor 15:7	applicability 11:3		
afraid 20:23 21:2	applicable 10:17 13:16		
afternoon 6:9	application 29:22 54:14,22 63:2		
agree 7:6 8:4 11:7,19 13:9,15	applications 29:24 36:7,11,12,21,23, 25 37:6,13,14,15,22 50:6		

THE SULLIVAN GROUP OF COURT REPORTERS

Index: bolded..contents

bolded 35:4,6,11	10:22	column 29:15 32:1,9,12,15 33:13 34:11,12,25 50:20,24 54:5 56:20,24, 25 57:11 58:3,17 66:1, 4,6,9	36:15
break 6:23 21:21 41:1,2,3,24 61:3	character 24:1 54:14,21	columns 29:10,13,16,18,19 30:1 31:25 32:24 65:22,24 66:2	concepts 16:24
breaks 6:20 7:2	characters 23:21	combination 17:5,14,23 18:10 19:15, 20,25 30:25	concluded 67:5
BRI 14:5,6 15:17,23 16:3,6, 21 22:18	chat 22:2	combine 17:10,19 18:4,24 19:3, 9,12 58:8	conclusion 19:19
briefly 12:2	check 6:12	combined 19:18	condition 21:3
briefs 8:21	choose 23:17 29:2	combining 19:8	conducted 9:22
broader 55:15 56:16	citation 44:4 46:3,6,25	comment 24:7	confer 9:11
broadest 14:14 15:13 16:12	citations 46:13,21	communicates 7:7	confidential 53:17
browsers 37:7	claim 17:6,7,15,23,25 18:8, 10,16 19:6,11 61:15,19 62:1 63:20	communication 9:16,17	configured 36:20
buy 60:16	claimed 17:11 58:11	compared 38:12	confirm 11:3,14 12:15 14:10 22:15 59:2
C			
calculation 42:23	claims 12:3 14:7,13 15:12,18 16:11 20:13 21:5,14 53:24 62:5	component 38:23 39:18,23 40:1,14, 22	Confirmed 22:21
call 9:6	claims' 21:11	computation 31:12	confusion 22:7 64:8
called 6:4 47:25 48:5 49:13,22 51:16	clarification 12:12 23:22 25:14 26:21 30:4 31:22 33:23 37:19 41:25 42:3,22 43:10,13 49:3 53:5 60:5 62:8 64:6	computations 31:3,5,8 64:24	consecutive 26:20,23
card 40:6,8,9,12,14,17	clarify 8:25 16:1 18:20 32:16 35:22 37:3,10 39:1 46:9	computer 27:20 28:11,15,16 29:6 30:11 33:16 36:19 40:6 42:20 43:14 65:13	consequence 47:3
card's 40:10	clarity 9:7	computers 28:12	considerable 10:8
careful 47:3	clause 47:6	conceiving 63:7	considered 15:23 16:3 20:14
case 19:8 24:25 25:3 40:21 42:18 43:8 51:17,23 55:10 57:23 60:19 65:1, 25	clear 55:7 62:7,9	conceived	consistent 43:3 44:25 45:6
cases 27:8 36:10,18 43:5	closed 45:18		consistently 61:22
change	colleague 41:14		consisting 23:7 24:10,16 25:20 42:8
			consists 25:23 29:2,3,16 31:21
			construct 33:4
			contents

22:10	couple 62:14	defeat 51:24	differences 11:21,24 12:2 13:21
context 29:24 48:14 63:2 64:9	court 12:12 23:22 25:14 26:21 30:4 31:22 33:23 37:19 42:22 49:3 53:5 60:5 62:8 66:15,19,21, 24 67:2	definition 26:4 30:3 65:20	differently 13:6 22:11
continue 41:23	cross-examination 7:8	degree 38:12	digital 54:11 55:1,11 58:19 59:11 60:4,6,23 64:18
control 35:25 40:4	crypto 23:18 25:1	denoting 49:25	digits 29:3 42:24
correct 8:9,10 9:19,20 15:15, 16,17,24,25 16:9,13,18, 19 18:3 19:18,21,22 20:16,17 21:18 22:20, 25 23:9,10,16 24:14 25:9 27:9,10 28:10 30:24 31:10,14,16,17 32:5,6,10,15,20 34:6,8, 9,13,14,16,19,20 35:1, 2,8,9,16,17 36:2 37:1, 16 38:7,8,9,17,24,25 39:7,23 40:23,24 42:12, 13 43:3,6,7,22,23 44:5, 6,7,9,16,17,23 45:4,5,8, 9,13,14,20,21 46:4,5, 11,12,14,21,22 47:1 49:23 50:25 51:1,9,10 52:6,17,20,21,24 53:10, 11,14,22 54:6 55:22 56:18,19,21,22 57:2,3, 6,9,10,13 58:6,11,12, 22,23,25 59:14,16,17, 19,20 60:25 61:1,10,11, 17,18,23,24 62:2 63:9, 10,21 64:24,25 65:2,7, 8,23 66:4,10,11	cryptographic 23:24 24:9 27:17 30:15 47:12 48:11,18 53:3 55:18	depend 19:19	disadvantage 31:8
corrected 45:23	cryptology 23:6 24:8,15,23 51:15, 20 64:16	depends 13:17 28:22 29:22	disadvantages 64:21
correctly 12:16 52:1 54:17	<hr/> D <hr/>	deposed 7:12	disclaimers 18:14,19
correlate 27:3	data 30:7,15,17 31:2,4,9,16, 18 34:4,15,17 44:22 45:2,3,8,11 47:14,15, 17,18 48:24,25 49:7,8 52:11,12	deposition 6:18 7:19 8:16,19,24 9:3,10,13,14,22 11:5,6	disclosed 17:8,17 18:1,9 58:8
correspond 62:23 63:8,12 64:19	days 10:11,14	derived 51:22	discloses 58:10,18 59:9
corresponds 33:5 63:5,6	decide 26:16 30:16	describe 46:24 54:19 55:20 58:24 59:15	disclosure 11:17,19 15:21 16:4 25:3 61:9,16,20
cost 60:13	declaration 6:15 7:20,21,25 8:8,9 10:1,2,5 11:7,12,15 14:2,4,24,25 16:17 22:8,10,12 34:2 38:14 42:4 46:2,7,13 58:14 61:7,8 62:4	describes 13:5 62:1 63:16	discuss 7:3 16:17
counsel 7:4 9:11,16,18,23 45:25 66:15	declarations 7:12 8:5,23 9:2,7 10:20	describing 56:17	discussed 11:16 13:22 16:20 22:9, 17,22 29:8 55:3,14 56:14 65:25
	decrypt 47:15,19	description 12:22 16:10 20:13 21:6, 10,13,15,17 48:22 51:7 61:13	discussing 22:16 65:19
	decryption 47:16 48:13,19,24 49:22 51:17,18,21,22 52:9	detail 59:2	discussion 12:21 13:8 41:10 62:4, 18
	deduced 34:5	detailed 50:12	discussions 42:3
		details 10:7 13:19 20:25 57:22	dispute 60:19
		determining 19:5	document 14:11,17 47:7
		device 30:8	documents 10:9
		devices 38:4	double-check 50:9
		difference 12:4,9,10,13 30:13 35:12 63:15,19	downloaded 22:4

downloading 22:3	encrypting 48:25 53:18 64:17	experience 11:9	11:17,18 13:9,10,14 20:13 46:16
draft 10:15 66:18	encryption 12:22 47:5,10,11,16,17, 19,21,22,23 48:1,4,5, 10,12,15,19,23 49:1,4, 6,7,12,13,17,18,19,22, 23 50:23 51:3,9,11,12, 14,16,17,18,21,23,25 52:2,3,4,7,8,10,12,15, 22,24 53:2,9,12,13,15, 20 54:23,25 55:4,6,8, 11,13,15,20,21,24 56:3, 9,15 57:2 63:11	expert 20:24	file 14:23 15:3,5 22:3,4,8,9
draw 35:14		expertise 19:13	filing 14:23
due 45:24		explain 60:9	find 50:17,18
duly 6:4		explained 12:5 53:1	fine 7:1 8:2 21:22 50:19
E		explicitly 57:9	finite 23:7 24:16,19 25:20,23 26:1,4,10 27:7,13 42:8, 9,10,20
earlier 6:18 9:22 11:4 22:10,12 42:7 44:25 62:18 63:14 64:20	end 28:12 30:13 34:3	expressing 49:9	flaws 36:18
easier 50:3	ends 16:2	extends 46:8	follow 50:7,8
easily 51:22	entire 15:21 16:4 46:7	extent 13:13	follow-up 63:23,25 64:2
easy 12:1 19:12 62:9	entities 36:6	F	form 28:14,19,20 39:6,11,12, 13,14,16,21 49:8 51:15 52:5 53:9
effort 10:10	entitled 61:9	fact 17:17	formulate 32:11
efforts 60:13	entries 29:3	factors 19:5	formulation 16:7
element 19:14,23 32:1,2,4,8,12, 22 66:9	entry 28:25 29:3 33:14	fair 31:11 36:22 46:23	forward 22:7
elements 17:8,11,17,25 18:8,16 19:12 25:16,17 32:4,17 42:10 57:18	environment 35:16,18,19,23	familiar 20:21	found 21:17 45:12 51:8
Ellison 13:23 46:15,17	essentially 53:8	faster 31:12	Friday 6:1
embodiment 54:10 57:13,15,20,21, 25 58:4,7	EST 6:1	features 62:1	froze 33:16
embodiments 57:24 58:1,8	exact 21:3	feedback 9:21	full 9:7 21:10 59:1
encrypt 47:14,19 49:8 52:11,12, 15	EXAMINATION 6:8 62:17 64:4	feel 6:22	fully 10:19 48:3 61:13
encrypted 12:17,18,21,24,25 13:3, 4 52:18,19 53:7	examples 34:5,10	fewer 31:3,4,8 36:6 38:13 64:24	G
	Exhibit 22:17 23:4 34:22	field 25:16 42:10	gave 27:1 43:10
	exist 63:8	figure 13:10,18 47:7 48:16	
	existence 18:17	figures	

THE SULLIVAN GROUP OF COURT REPORTERS

Index: general..key

<p>general 6:19 48:11,18 50:4</p> <p>generally 47:9 63:7</p> <p>generated 58:20 59:11</p> <p>generating 64:17</p> <p>generic 55:4</p> <p>give 6:23 21:2,13,14 26:4 29:23 33:16 37:17</p> <p>giving 36:19</p> <p>goal 30:19</p> <p>good 6:9,11 41:2 60:15</p> <p>great 8:3 15:5 21:23 22:5 23:2 41:5,12,23 66:13, 18 67:3</p> <p>ground 20:19,20,22 21:4</p> <p>grounds 20:7</p> <p>group 25:16</p> <p>guess 16:7 20:25 27:2,11 34:21 40:13 56:5</p> <hr/> <p style="text-align: center;">H</p> <p>happen 45:25</p> <p>happening 36:14</p> <p>happy 43:9</p> <p>hard 29:21 33:3</p> <p>heads-up 6:24</p>	<p>hear 33:15,18</p> <p>heard 55:5</p> <p>held 9:15</p> <p>Henry 41:17,18,21 62:14,17 63:22,25 66:14,21,23 67:1,3</p> <p>hereinafter 54:15</p> <p>high 13:19</p> <p>higher 35:24</p> <p>highest 35:20,21 36:5 38:6,12</p> <p>history 15:22 16:5,11</p> <p>hope 6:9</p> <p>hour 41:1</p> <p>Houston 6:22</p> <hr/> <p style="text-align: center;">I</p> <p>ID 50:22 54:13,23,24 55:5, 8,10 56:9 57:1</p> <p>identical 11:22,23</p> <p>identification 33:19 54:21</p> <p>identifies 54:22</p> <p>identify 32:21 66:2,3</p> <p>identifying 54:14</p> <p>imagine 40:3,5</p> <p>implement 64:15</p>	<p>important 19:14 23:5</p> <p>include 20:7 46:13</p> <p>including 15:21 16:4 47:4</p> <p>index 28:24 29:14,17 32:23, 24 66:3</p> <p>indicating 21:5 66:5,6,8</p> <p>information 32:14 35:24</p> <p>infrastructure 60:16</p> <p>innovative 19:10</p> <p>inoperable 20:1</p> <p>insert 40:6 45:19</p> <p>integer 26:20,24</p> <p>integers 66:11</p> <p>integral 43:21,25 44:2,8,11,15</p> <p>intended 20:1 27:18 45:23</p> <p>interested 31:12</p> <p>interpret 14:6 15:18 39:8</p> <p>interpretation 14:14 15:13 16:12 43:8</p> <p>interpreted 16:6</p> <p>interpreting 44:12</p> <p>invalid 21:17</p> <p>invent 23:17,24</p> <p>invention</p>	<p>19:10 54:12 57:25</p> <p>inventive 19:15,20</p> <p>involved 19:20</p> <p>ios 38:5</p> <p>IPR 8:8 16:21 20:4</p> <p>IPR2022-00113 7:17</p> <p>italicized 35:3,6,7,10</p> <p>item 30:7,17</p> <p>iterations 43:16</p> <hr/> <p style="text-align: center;">J</p> <p>Jacob 41:15,18 62:13</p> <p>Jeremy 41:14</p> <hr/> <p style="text-align: center;">K</p> <p>kernel 36:13,18</p> <p>kernels 36:17</p> <p>key 12:5 23:18 24:4 25:7 27:18 30:16 35:13,15 38:22 39:16,22 40:2,3, 10,11,12,15,19,23 43:20,24 44:1,7,11,15, 22 45:1,3,7,11 47:5,10, 11,15,17,19,20,21,22, 23,24 48:1,4,6,10,11, 15,19,24 49:1,4,6,7,11, 12,13,17,18,21,23 50:4, 5,23 51:3,5,9,11,12,13, 14,15,17,18,21,22,23 52:3,5,8,10,12,15,16, 18,19,22,23 53:2,7,8, 12,15,20,23 54:1,3,8, 15,19,22,23,25 55:3,4, 6,8,11,13,15,18,20,21,</p>
---	---	--	---

THE SULLIVAN GROUP OF COURT REPORTERS

Index: keys..obvious

<p>22,23,24 56:2,3,9,15 57:2 58:10,20,25 59:11, 16,18,22,24 60:10,24 63:11 64:17</p> <p>keys 12:8 23:6,11,25 24:10, 14,15,23 50:13 52:13 60:16,21</p> <p>Khan 6:8 12:19 21:21,23 22:1 24:3 25:18 26:25 30:5 31:23 34:1 37:23 40:25 41:5,7,11,14,20,22 43:1 49:10 53:6 60:8 61:3,6 62:11 63:23 64:2,4 66:13,17,20</p> <p>kind 36:19 44:12 52:11 55:3</p> <p>knowledge 34:17</p> <hr/> <p style="text-align: center;">L</p> <p>language 19:2 23:19,25</p> <p>leaves 51:4</p> <p>legal 10:17 16:17,24</p> <p>legislation 21:1</p> <p>length 33:6</p> <p>level 13:19 36:3,5 38:6,10</p> <p>levels 38:12</p> <p>lies 63:19</p> <p>limit 37:24</p> <p>limitation 61:13</p> <p>limitations 61:15,20</p> <p>linear 29:11</p>	<p>lines 34:11,12 35:1 50:20,24 56:20,24,25 57:11</p> <p>link 14:19,22</p> <p>Linux 37:18,21</p> <p>list 28:23</p> <p>load 28:14</p> <p>location 53:21</p> <p>long 10:4 27:12</p> <hr/> <p style="text-align: center;">M</p> <p>machine 37:5</p> <p>machines 37:17,18,20,24</p> <p>macos 37:18,20 38:1</p> <p>made 7:12 10:19 44:5 51:24</p> <p>make 41:8 44:10 45:10 46:24 53:1</p> <p>makes 13:18 50:11</p> <p>manner 7:7 58:10</p> <p>mapped 63:1</p> <p>mapping 63:3</p> <p>mathematics 25:13</p> <p>matrix 29:12</p> <p>matter 21:11 57:17</p> <p>meaning 45:6</p>	<p>means 35:22,23 37:6 39:3 42:18 43:11 53:1,16 57:16,22</p> <p>meant 39:6 55:24 56:4</p> <p>mechanism 32:21</p> <p>medication 6:14</p> <p>meeting 9:12</p> <p>memory 12:6,7 40:22 53:19</p> <p>mention 7:24 17:4 34:10 35:15</p> <p>mentioned 13:20 18:7 28:18 30:20 31:15 37:9 42:7,14,19 64:22</p> <p>merchant 60:15,17</p> <p>merchants 60:16</p> <p>micro 37:25</p> <p>million 28:25 29:2 30:2</p> <p>mind 22:3</p> <p>misheard 65:18</p> <p>mobile 38:4</p> <p>model 60:12</p> <p>Monaldo 41:14</p> <p>Monday 9:12</p> <p>morning 6:11 63:14</p> <p>moving 22:7</p>	<p>Muir 46:15</p> <p>multiple 31:21,24 47:23,25 57:23 58:1</p> <hr/> <p style="text-align: center;">N</p> <p>natural 19:7 23:25 28:23</p> <p>necessarily 12:6,16,18,20 26:13</p> <p>note 12:15 41:8,9 61:12</p> <p>noted 14:4</p> <p>notes 37:6</p> <p>November 6:1</p> <p>number 14:17 20:25 21:2 24:19 32:14,15 33:19 42:11, 20 50:22 54:13,21,23, 24 55:8,10 56:9</p> <p>numbered 22:11</p> <p>numbers 7:16 26:1 42:9 46:15,17</p> <hr/> <p style="text-align: center;">O</p> <p>oath 8:13,15,16</p> <p>object 24:5 25:8,12,15 26:5</p> <p>objects 23:8,12,15 24:11,17,24 25:11 28:13 42:9</p> <p>observing 41:19</p> <p>obtain 17:11 18:16</p> <p>obtained 47:2</p> <p>obvious 17:8,25 18:8,10 19:6,11</p>
---	--	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: obviousness..prevent

44:14 45:13 51:8 55:21 57:4 58:9	overlaps 8:5	20 13:10,11,15,16 14:13 15:12 16:10 20:10 21:10,13 25:4,6,7 27:4 34:12,18 35:1 38:18,20 39:8,20 41:16, 17,19 44:13,22 45:13 47:7 48:14,23 50:7,20 54:4 55:7 56:6,8 57:9, 17,18 58:5,9 61:9,14, 16,20,23 62:1,5,7 63:15 64:10,11,15 65:1,4,22 66:8	22:8
obviousness 16:22 20:2,7,9,14 22:23 44:13 61:21	owner 7:13 41:19		PGR2022-0007 7:17,22
occurrence 43:9	owner's 41:16,17		PGRS 20:19
occurrences 50:17	P		Phillips 15:7
one-to-one 63:3	paper 42:24 48:8		phrase 16:2 18:23 43:16 57:12
onwards 57:12 58:4,18	paragraph 14:2,10,12,13 15:5,9, 12,20 17:4,24 18:7 19:24 22:19 23:4,5 24:15 34:2,7,21 35:14 38:14,17 39:19 41:24 42:4,6 43:17,20 44:4, 18,21 45:15,18 46:3,8 54:4,7,9,18 55:9,12,20 56:10,14,17 57:11,19 58:14 59:1 61:12,25	patent's 15:21 16:4	piece 40:16
open 14:1 15:3 22:14 51:4	paragraphs 16:15,16 22:11,16,17, 18,24 23:1 46:12,23	patents 10:9 11:22,25 12:9 46:16 47:4 48:10 55:16 57:23 58:1 63:19	places 42:5,15 65:4,6,9
opened 14:11	parentheses 45:19	pattern 27:2,4,8,12,17	point 7:7 23:6 28:16 34:10 46:14 50:13
operate 60:16	part 32:9 43:21,25 44:2,8, 11,15 54:12,20 55:10	people 36:15 55:23	points 35:13,15 46:25
operated 36:20	part-time 15:6	perform 31:7 47:21 48:5 49:12, 19 52:23 60:19 64:24	POSITA 17:19 18:4,15 19:14
operating 36:15 37:5 38:1	parties 53:19	performed 53:9,13	position 23:11
operation 49:1	parts 10:15 34:18	performing 30:24 31:12 48:19	potentially 28:7
operations 25:17	party 58:19,21,24 59:10,12, 16,19,21,23,24,25 60:1, 7,11,14,19,20,23	performs 49:11,22	predetermined 39:10
opinion 25:8 49:17,18	pass 63:22	period 9:18	prefer 36:4
order 32:13,16,17 60:13	passage 58:18,24 59:9,15	periodically 6:21	preferably 50:21
ordinary 17:10 18:24 19:3 45:12 51:7 57:5 61:10,14	passages 34:15 57:6	person 17:10 18:23 19:2 30:8 45:12 51:6 57:5	preferred 49:15,25 50:2
organize 36:1	patent 7:13,14 8:24 9:2 11:17, 20	petition 20:3	Preneel 6:3,9 14:25 22:2 41:18 62:15 64:5
organized 29:11,12		Petitioner's 41:13	preparation 8:24 9:2,10
Outsource 60:6		petitions 20:4,7	preparatory 9:12
outsourcing 60:3		PGR 7:21 8:7 14:11,14,25 15:13 16:21 20:4 21:4	present 54:12
overlap 10:25			pressure 45:24
			prevent

THE SULLIVAN GROUP OF COURT REPORTERS

Index: previous..request

6:14	12:7 53:16,18,21	readily 61:15,19	referring 7:20
previous 13:20 22:9 24:7	protection 12:11,14	reading 34:6 57:5 61:22	relate 11:5
previously 39:4	provide 6:20 21:10,16 38:18,20 39:9,15,20 46:1 59:24 60:10	reads 14:13 15:6,21	related 12:10 22:18
prime 42:9	provided 9:21 10:10,18 43:13 54:10 59:18	real 36:12	relates 12:13
principle 33:4	providing 58:25 59:16,21	realization 57:16	remain 53:17
prior 17:9,18,20 18:1,9 19:5 20:15 61:22	public 51:11,14,18,24 52:3,4, 5,8 53:1	reason 9:6 17:9,18 18:4,16,23 19:2 26:16 35:10	remarks 10:21
private 12:5 23:6,11,18 24:4, 14,15,23 25:7 38:22 39:16,22 40:2,3,10,11, 15,19,23 43:20,24 44:1, 7,10,15,22 45:1,3,7,10 50:22 51:3,8,12 52:8, 16,18,19,22,23,25 53:7, 8,12,15,16,17,20,23 54:1,3,8,15,19,22 55:21 56:2 57:1 58:10,20,25 59:11,16,18,21,24 60:10,24	purpose 20:1 21:12 48:23 50:4,5 51:24	reasonable 14:14 15:13 16:12	remember 62:19,21 63:17,18
privilege 35:20,21 38:7	purposes 7:19 47:24,25 51:3	recall 21:7	render 19:25
privileges 36:3,5	Q	recess 21:24 41:6 61:5	renders 19:6
proceeding 7:16	question 8:7,25 13:17 17:12 18:22 24:18,21 27:25 29:21 33:3,7,8,9 48:2,4 54:16,18 59:6,7	recited 34:18 53:24 54:4	repeat 13:1 17:12,16,21 30:20 33:7 43:9 48:2 54:16 56:1 59:5
proceedings 7:21 8:21 9:15 67:5	questioning 6:24 59:8	recites 34:15	repeating 11:1
process 40:4	questions 6:19 11:2,3,4,8,11 13:14,16 62:11,15 63:24 64:1,3 66:13,14	recognize 61:15,19	rephrase 36:4 37:2 49:5
processing 35:16,18,19 37:7 38:11	quote 19:1	recollection 10:6	reporter 12:12 23:22 25:14 26:21 30:4 31:22 33:23 37:19 42:22 49:3 53:5 60:5 62:8 66:15,19,21, 24 67:2
processor 35:19 36:1	quoted 34:15	record 41:10,12 66:16	represent 23:20,21 24:1,19 28:6, 13 29:6 42:19
processors 38:13	quoting 34:25	redirect 62:13	represented 23:13 24:12 25:10 27:24 28:2,9 29:7 30:12 32:6 42:10 65:12
properly 36:20	R	reduce 60:13	represents 26:23
prosecution 15:22 16:5,11	re- 43:15	refer 7:20 46:15 47:6,8 55:23 56:2,3 61:25	reproduce 21:3
protected	read 39:5 54:9 59:1,4	reference 13:23,24 46:17	request 6:21,23 36:12 39:25 40:7
		referred 54:15	

THE SULLIVAN GROUP OF COURT REPORTERS

Index: requested..starts

requested 12:12 23:22 25:14 26:21 30:4 31:22 33:23 37:19 42:22 49:3 53:5 60:5 62:8	66:2	session 11:2	smart 40:6,8,9,10,12,14,17
requesting 38:22 39:17,22 40:21	rules 50:6,7,8,10	set 30:12	software 12:11,14,16 33:19 36:11,18 38:19,21,23 39:9,15,17,21,23,25 40:1,7,13,16,20 43:21, 25 44:2,8,12,16 50:21, 22 51:4 54:10,13,20,23, 24 55:5,7,10 56:9,18 57:1
requests 66:16	running 28:24 36:13	shape 28:14,19,20	software's 40:11,19
require 19:15	S	share 10:25	solemn 8:16
requirements 27:12,16	scientific 48:8	shared 22:2	sound 8:1
requiring 21:10	Scott 41:19	short 31:3	sounds 67:3
Research 15:7	scratch 38:19	shows 13:18	speak 9:7 37:3 40:14 64:9
respect 7:14 9:22 10:20 11:12 13:8,14 30:13 62:7,9,10	secret 51:19	sic 44:21 64:6	speaking 6:15
responses 7:14	section 35:3 46:7,13 61:7	sic] 42:11	specific 13:17 28:22 29:8 46:15 47:6 48:8 57:16 63:2
restart 59:8	secure 12:7	side 41:13,17	specifically 6:21 7:24 55:1 64:10
restricted 36:25 38:10,11	securely 12:8	signature 54:11 55:2,11 58:20 59:11 60:4,6,18,23 64:18	specification 11:1 15:22 16:5
returning 61:7	selected 28:23	signed 58:19 59:10	specifics 6:20
review 8:23 9:1 20:3,25	sells 60:15	signing 54:11 55:1	spent 10:8
reviewing 16:10	sense 12:4 17:3 36:5 38:10 55:16 56:16	simple 40:5	standard 14:5,6 15:18 16:12 19:13 20:10,14,15 22:23 24:8 44:13 61:23
ring 25:16 35:15,18 36:2,8, 13,21,25 37:8,14,16,22 38:7,11,12	sensor 37:5	simpler 36:24 37:3	standards 10:17 16:18,21 22:18 24:9
rings 35:24 38:10	sentence 15:20 16:2 19:24 34:6 35:4,5,7 42:6	simplified 36:17	start 6:19
rough 66:18,22,24	sentences 35:6,7	single 25:22 33:12 34:14 46:25 57:24,25	starting 61:8
row 29:15 32:1,9,12,14 33:12 66:1,4,6,8	separation 36:16	situations 37:11	starts
rows 29:9,12,16,17,19 30:1 31:25 32:23 65:22,24	sequence 25:20 26:1,4,10,23 27:3,6,7,13,15	skill 17:10 18:24 19:3 45:12 51:7 57:5 61:10,14	
	sequences 23:7 24:16 42:8	slight 22:6	
	serial 50:22		

THE SULLIVAN GROUP OF COURT REPORTERS

Index: state..truth

57:12	14 66:12	57:16 65:13 66:3	terms 34:4 62:20
state 23:5 34:3 44:21	structural 27:11	systems 25:1 36:16,17,23,24 37:3,4,5,15,21 43:14	testified 6:6
statement 44:5,10,25 45:10 48:7 58:14,15	structure 25:25 26:6,12,14,18 27:2 29:8	T	testifying 8:17
statements 7:12 10:21 47:2	study 47:3	table 28:13,17,18 29:2,9,11, 14,16,20,23 30:1,2,10, 11,17,22 31:2,6,7,13,20 32:2,3,10,18,21 33:5, 12,13,20,21,22,25 62:25 63:1,5,6,13 64:12,19,23 65:5,6,10, 12,21 66:7,10,12	testimony 7:4,9 8:4,12,13,20 9:21
states 15:12 17:25 38:17 43:20	studying 10:9	tables 27:22,25 28:2,8,10,21 29:25 30:6 33:2,10 62:19,23 63:2,4,9 64:7, 13,22 65:3	text 10:14
statute 21:9	subject 21:11	takes 10:14	textbooks 24:10 25:2
step 18:13 19:10,16,20	submitted 7:13,21 10:2 46:2	talk 41:15	things 19:8,9 30:14 36:13 47:1
stings 23:20	subparagraph 34:21	talked 42:7 64:6,20	thousand 30:1
storage 40:22 58:21 59:13	subsequent 8:20	talks 65:4	time 10:8 41:2 45:24 46:10 50:15 59:3,4
store 31:2,4,9,15,19,20 32:2, 17 60:16,17	substance 7:3	teach 55:7	today 6:14 7:4,9,12,19 8:12, 16,20,24 9:3,8,10,15 11:5,12 41:8 66:18
stored 12:6,8 40:12,16,19 53:21	substantial 12:4,8	teaches 55:9	tools 37:7
stores 58:19 60:23	substantiated 21:15	technical 20:24 46:25	traditional 64:16
storing 40:23 53:18 59:10	substantively 8:5	technically 43:12 44:1 45:2	transaction 58:19 59:10,22,23,24, 25 60:10,11,14,18,23
stream 65:18	subtle 13:20	techniques 21:1	transactions 60:17
string 24:5 25:6,8,10,19,20,22 26:8,9,10,18,19,22 27:6,14,16,20 28:15,16 29:1 30:10,16,23 31:4 32:2,4,7,22 33:6,12 42:11 54:14,21,24 63:1, 5,6,12 64:18 65:5,13, 14,17,19 66:5,6,8,9	sufficient 18:18 33:6	ten-minute 41:3 61:3	transcript 66:15
strings 23:7,12,15,21 24:2,11, 12,16,20,24 27:23,24 28:1,3,10,12,24 29:7 30:3,12 31:21,24 32:18, 25 33:2,9 34:4 42:21 62:18,23 63:4,7 64:12,	summarized 60:3	term 40:13 42:1,5 45:6 48:8, 11 53:2,15,23 54:1,3 55:4,14,15 56:15	trial 8:17,20
	support 7:13	terminology 49:15	trouble 67:1
	supported 61:13		true 63:20
	suppose 24:13		trusted 60:7
	sworn 6:4 8:13		truth 6:5,6
	symmetric 51:20 52:2 64:15		
	system 23:18,24 38:1 54:11		

<p>TTP 60:4</p> <p>Tuesday 9:15 11:6,13,18 13:24 16:20,25</p> <p>turning 10:1 14:2 23:4 38:14 44:18</p> <p>two-minute 21:21</p> <p>type 19:19 28:20 29:19 33:1</p> <p>typical 37:11</p> <p>typically 25:13 29:20,22 31:19 36:8,9,15 37:4,10 66:3</p> <p>typo 45:22</p> <hr/> <p style="text-align: center;">U</p> <p>unauthorized 53:19</p> <p>undefined 38:21 39:1,3 42:1</p> <p>understand 7:2,5,11 8:12,14,15,18, 19,22 15:23 16:3 20:8 21:12,16,19 24:13,22 35:11 42:16 55:24 56:3 62:10</p> <p>understanding 9:20 10:17 16:21,23 17:1,22 20:6 39:7 47:9 57:20 58:2</p> <p>understood 10:19 50:1 52:1 57:1</p> <p>unique 50:22</p> <p>USC 20:19,21</p> <p>user 36:7,16,20,23,24 37:6, 12,14,15,22</p> <p>user-operated 36:11</p>	<p>users 36:19 37:4</p> <p>Usman 41:14</p> <hr/> <p style="text-align: center;">V</p> <p>values 30:2 66:12</p> <p>verification 60:3,7,20,21</p> <p>verify 47:18 60:17</p> <p>versa 65:9</p> <p>versus 30:10</p> <p>vice 65:9</p> <p>view 13:19 44:13 45:13 51:8 61:21</p> <p>views 11:16,19,23 13:22,23 16:23 17:1</p> <p>virtual 40:14,17</p> <p>visit 43:16</p> <hr/> <p style="text-align: center;">W</p> <p>wanted 6:12 17:4 35:14 42:2,15 56:5 62:24</p> <p>Ward 7:4 41:19</p> <p>Ward's 7:13 9:11,16,18,23</p> <p>washing 37:5</p> <p>ways 28:7,9 30:19,21,23</p> <p>week 6:18 9:23</p> <p>whichever</p>	<p>40:22</p> <p>Window 37:24</p> <p>Windows 37:17,20</p> <p>word 24:22 36:9 37:7,10 42:14 43:4 63:16 65:18</p> <p>words 16:1 23:19,25 24:1 34:15 42:15 45:18 64:8</p> <p>work 6:25 10:7 18:13 40:6 42:24</p> <p>working 10:11</p> <p>wrap 6:24</p> <p>write 10:2,4 28:11 39:5 48:7</p> <p>writing 10:14</p> <p>written 20:13 21:5,10,17 61:13</p> <p>wrote 10:13</p> <hr/> <p style="text-align: center;">Y</p> <p>year 10:7</p> <hr/> <p style="text-align: center;">Z</p> <p>zeroes 23:8 24:17 25:21,24 26:1,4,10,17 27:7,13,16 42:8</p>
--	---	---