

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 1, 2022

Page 1 - 103

8:06 a.m. EST - 11:48 a.m. EST

REPORTED BY:

Tamara L. Houston

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

Job Number 22-117173

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 8:06 a.m. EST to 11:48 a.m. EST, Tuesday, November
1, 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 1000 Maine Avenue SW
7 Suite 1000
8 Washington, DC 20024
9 (202) 626-6383
10 khan@fr.com

11 On behalf of the Patent Owner and Witness:

12 RAMEY LLP
13 BY: JACOB B. HENRY, ESQ.
14 5020 Montrose Boulevard
15 Suite 800
16 Houston, Texas 77006
17 (832) 454-1456
18 jhenry@rameyfirm.com

19 ALSO PRESENT: Scott Ward, Proprietor
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.....	91
Mr. Khan.....	97

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 1, 2022

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

EXHIBIT	DESCRIPTION	PAGE
---------	-------------	------

None.

--o0o--

THE SULLIVAN GROUP OF COURT REPORTERS

1 Tuesday, November 1, 2022, 8:06 a.m. EST

2 --o0o--

3 All counsel present stipulate
4 that the witness shall be sworn remotely
5 by the court reporter

6 * * *

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

12 EXAMINATION BY MR. KHAN:

13 Q. Good morning. Thank you very much,
14 Dr. Preneel.

15 MR. KHAN: Jacob, thanks.

16 BY MR. KHAN:

17 Q. I wanted, I guess, to first start off with
18 asking you if I'm pronouncing your name correctly.

19 Is it Dr. Preneel?

20 A. That's correct. Yes.

21 Q. Great. I'm joined here by my colleague,
22 Jeremy Monaldo, also with Fish & Richardson.

23 MR. KHAN: Jacob, is there anybody else at
24 your end who is participating or listening to the
25 proceedings, just for the record?

THE SULLIVAN GROUP OF COURT REPORTERS

1 MR. HENRY: Mr. Scott Ward is present.

2 MR. KHAN: Okay. Fantastic.

3 So from Petitioner's side, there is Usman Khan
4 and Jeremy Monaldo with Fish & Richardson. And from
5 patent owner's side, we have their expert, Dr. Preneel;
6 the attorney, Mr. Jacob Henry; and patent owner, Scott
7 Ward.

8 Is that correct?

9 MR. HENRY: That's correct.

10 MR. KHAN: Okay. Thank you.

11 BY MR. KHAN:

12 Q. So, Dr. Preneel, I'll start off with some
13 general questions, getting to specifics, but I'll be
14 providing periodic breaks as we go. So, you know, you
15 don't have to go through it -- through without any
16 breaks. You know, you may request a break at any time.

17 MR. KHAN: And, Tamara, yourself as well, if
18 you need a break, please let me know.

19 BY MR. KHAN:

20 Q. I just request that you let me know about five
21 minutes ahead of time or so, a few minutes ahead of
22 time, so that I can wrap up my line of questioning or I
23 at least know when to stop.

24 Does that work for you?

25 A. That's fine.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Great.

2 And during the breaks, do you understand that
3 you are not allowed to discuss the substance of your
4 testimony today until your cross-examination is
5 concluded?

6 A. I understand that.

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

11 A. I agree.

12 Q. Thank you.

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

15 A. I understand that, yes.

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

19 A. I understand that, yes.

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

23 A. I understand that, yes.

24 Q. And do you understand that you're being
25 deposed today for statements made in your declaration

THE SULLIVAN GROUP OF COURT REPORTERS

1 submitted in support of the '766 patent owner response?

2 A. Yes, I understand that.

3 Q. Do you have a copy of the exhibits that were
4 cited in your declaration and a copy of the patent owner
5 response?

6 A. I do have all these documents in digital
7 format. I don't have them all printed out.

8 Q. Okay.

9 A. But I do have a digital format. I can find
10 it, like, if you give me the correct document. But I do
11 have in front of me the patents and my declaration and
12 also the declaration of Dr. Black.

13 Q. Okay. Fantastic.

14 So if I -- I'll refer to the documents either
15 by their exhibit numbers or their names. So if you're
16 not clear, please let me know.

17 A. That's fine.

18 Q. Great. Thank you.

19 Before we get started, is there any edit or
20 change that you'd like to make in your declaration?

21 A. Not at this stage, no.

22 Q. Okay. Fantastic.

23 So let's turn to your declaration. That's
24 Exhibit 2009 in the proceedings. And please let me know
25 when you have that in front of you.

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I have it in front of me. That's fine.

2 Q. Great. Thank you.

3 The cover page of your declaration states that
4 this declaration is for US Patent 11,603,766; is that
5 correct?

6 A. That's correct.

7 Q. Is it correct that that patent number is a --
8 includes a typographical error? The patent number that
9 you're referring to is Patent 11,063,766, which is also
10 Exhibit 1001?

11 A. Yes, that's correct. I see this now. Yes.
12 That's a typo. I confirm that.

13 Q. Thank you.

14 And in the header of the cover page and the
15 rest of the pages, you also list the patent number with
16 the same typographical error; is that correct?

17 A. That's correct, yes.

18 Q. Okay. And did you review your declaration and
19 the documents in preparation for this deposition today?

20 A. Yes, I did.

21 Q. Did counsel tell you how to answer questions
22 in your preparation?

23 A. Counsel told me to tell the truth.

24 Q. Have you been deposed before?

25 A. Not in a patent procedure. I've been a

THE SULLIVAN GROUP OF COURT REPORTERS

1 witness in an international arbitration.

2 Q. And how many times have you served as a
3 witness?

4 A. In arbitration, only once.

5 Q. And in the arbitration, did you have to be
6 deposed?

7 A. Yes.

8 Q. Was it one time or multiple times?

9 A. It was one time. It was a very long session.

10 Q. Okay. So is it correct that you've been
11 deposed once before in an international arbitration
12 matter but never for a patent-related matter? Is that
13 correct?

14 A. That's correct. That's correct.

15 Q. Have you been involved in any other patent
16 matters?

17 A. I'm the inventor of five patents.

18 Q. Okay. And have you --

19 A. And I've also -- I've also consulted several
20 companies on patent questions.

21 Q. Have you been involved in any other IPR
22 proceedings?

23 A. Well, for example, I don't -- I'm not sure I
24 fully understand what you mean. But, for example, of
25 course, my research --

THE SULLIVAN GROUP OF COURT REPORTERS

1 (Court reporter requested clarification.)

2 THE WITNESS: In my research, I've been
3 producing a lot of IPR because we've enjoined projects
4 with the companies and other institutions, and so I've
5 been running very large projects with up to 30 partners,
6 and those projects always had IPR clauses and, of
7 course, also during the running of the projects, so my
8 IPRs have come up.

9 BY MR. KHAN:

10 Q. I see. So let me clarify my question, please.

11 Have you been involved in other post-grant
12 patent matters?

13 A. I have not been in procedures before except
14 this procedure we're now in, but I've been -- as I
15 mentioned, I have been advising companies of the
16 original patents -- the applicability of patents and how
17 to -- where the patents would apply to their specific
18 case or how they could avoid patents in implementation.

19 Q. Okay. And just for clarification, in
20 subsequent questions if I ask you "IPR," that would mean
21 inter partes review, not intellectual property rights.
22 My apologies if there's any confusion.

23 A. My apology.

24 Q. So in paragraph 18 of your declaration --
25 could you turn to where it's paragraph 18, please?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Yes.

2 Q. So could you just read your paragraph 18 for
3 me, please?

4 A. "I have served as expert witness in several
5 IP-related court cases, both in Belgium and abroad."

6 Q. Yeah. So could you maybe clarify that
7 statement, so what you meant by "several IP-related
8 court cases"?

9 A. Well, I first -- the court case in the
10 arbitration, this was definitely IP-related, but I've
11 also been involved in a few Belgium court cases related
12 to copyright issues. Also, like, intellectual property
13 played a role.

14 Q. So is it correct to say that the IP-related
15 court cases, other than the arbitration one, were not
16 patent-related? Is that correct?

17 A. That's correct, yes.

18 Q. In your declaration, you -- in paragraph 10 of
19 your declaration -- and let me know when you get there,
20 please.

21 A. Yes.

22 Q. In paragraph 10, you start out the paragraph
23 by saying you are a "technical expert in the subject
24 matter areas relevant to this matter, including the
25 design and evaluation of cryptographic algorithms and

1 protocols, including cryptanalysis, security reductions
2 and proofs, cryptographic hardware and software, secure
3 execution environments, and secure electronic
4 transactions."

5 Did I read that correct?

6 A. That's correct.

7 Q. Is it your opinion that the '766 patent is
8 related to each one of these topics that you've
9 mentioned here? For example, the "cryptographic
10 algorithms, protocols including cryptanalysis, security
11 reductions and proofs, cryptographic hardware and
12 software, secure execution environments, and secure
13 electronics transactions"?

14 A. Well, the Patent '766 does not discuss in
15 detail cryptographic algorithms and protocols, and it
16 doesn't discuss security reductions and proofs. But, of
17 course, these are like basic signs you need to master to
18 understand fully this patent and to understand the
19 field. But the focus of this patent is indeed
20 cryptographic hardware and software, secure execution
21 environments and secure electronic transactions.

22 (Court reporter requested clarification.)

23 THE WITNESS: Secure execution environments
24 and secure electronic transactions.

25

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. So can you -- so in -- in this sentence, you
3 mentioned that the subject matter areas are relevant,
4 but could you explain to me how cryptanalysis is
5 relevant to the '766 patent?

6 A. Because if you want -- it's important to
7 understand cryptanalysis because if you want to
8 understand whether the cryptographic algorithms and
9 protocols are secure, and they are used in this scheme.
10 For example, if you look at the related patent LSM, it
11 actually uses hash functions, for example.

12 (Court reporter requested clarification.)

13 THE WITNESS: Cryptographic hash functions.

14 So cryptographic schemes are being used to
15 implement those secure transactions schemes. And, of
16 course, the goal of the patent is not to cryptanalyze or
17 break cryptographic algorithms, but it's important to
18 understand the strengths and weaknesses and limitations
19 to be able to fully understand how a patent -- the
20 patent works.

21 So I do believe that most of cryptography is
22 plain portion to understand the patent and that
23 cryptography consists both of design and analysis, and
24 those are two sides of one coin. And without
25 cryptography, it would not be possible to build some of

1 those systems.

2 BY MR. KHAN:

3 Q. Is there a difference between cryptographic
4 algorithms and protocols and cryptanalysis?

5 A. Yes, there is a difference, but they are two
6 sides of one coin. The cryptographic algorithm is a
7 mathematical operation in which we take a bit string and
8 you transform this to another bit string possibly under
9 control of a key. Cryptographic protocol is an
10 interaction between two or more parties in which you try
11 to achieve specific security goals within a secure
12 transaction, and again, cryptographic protocols
13 typically use cryptographic algorithms as -- through the
14 parties, and cryptanalysis is the science that studies
15 the security of algorithms and protocols. But you can't
16 have one without the other. They're two sides of a
17 coin.

18 Q. How are --

19 A. In order to be able to design and appreciate
20 the security of the system, you need to also understand
21 how they are being broken.

22 Q. How is -- or how are security reductions and
23 proofs relevant to the '766 patent?

24 A. Well, of course, this is the academic
25 discipline in which you study these algorithms and

1 protocols. These are tools and techniques which are
2 also mastered for this specific patent. Those
3 techniques have not been used because in the patent,
4 again, as I said before, you use building blocks to
5 build a larger system. But if you want to establish
6 security carefully, it's important that you can perform
7 such reductions and proofs, that you master those
8 techniques.

9 Q. And so are you saying that security reductions
10 and proofs is essentially an academic area that is
11 tangentially related to the subject matter here? Could
12 you clarify that, please?

13 A. I think these are toolboxes developed by
14 academia which I use to study these protocols and
15 algorithms, and I believe they give us new insights in
16 how to study them.

17 Q. Can you --

18 A. The academic relevance, I think today, if you
19 look at cryptographic standards today, it is -- both for
20 algorithms and protocols, it will be required that there
21 are security reductions and proofs in those.

22 Q. Can you give me an example of how the '766
23 patent uses security reductions and proofs?

24 A. The '766 patent does not secure -- use
25 security reductions and proofs, but to be able to fully

1 understand and evaluate the security today, I believe
2 it's essential that you also understand how security
3 reductions and proofs work and how you can prove how the
4 different components result in a secure system.

5 Again, it's two sides of the coin, and I fully
6 agree with you that to design a system, you don't
7 necessarily need to use the reductions and proofs. But
8 to study and understand the system, you would need
9 those.

10 But, of course, in the specific question we're
11 discussing here with this patent -- whether something is
12 patent or not or whether patent applies to something,
13 you don't need security and proofs. It's to understand
14 the security of the schemes.

15 Q. I'm sorry. Can you repeat the last sentence
16 you just said?

17 A. To decide on the question whether Patent A or
18 B are overlapping or not overlapping or innovative or
19 apply to a certain system, you don't need security
20 reductions and proofs. But to fully understand content,
21 you do need to understand security reductions and
22 proofs. And for this, I believe it -- my skills in this
23 area as expert are relevant to this general area in
24 which the patent is situated.

25 Q. So is it your position that the '766 patent

THE SULLIVAN GROUP OF COURT REPORTERS

1 claims have nothing to do with security reductions and
2 proofs; it's just for general understanding of the
3 subject matter?

4 A. It's for general understanding of the subject
5 matter, but also to specifically if you want to study in
6 detail how the components fit together, you would be
7 able to use security reductions and proofs.

8 Q. I'll repeat my question.

9 Is it your position that the '766 claims have
10 nothing to do with security reductions and proofs and it
11 is just for understanding of the subject matter?

12 A. I'm not sure I fully understand your question,
13 what is defined by "subject matter." I mean, the matter
14 of the patent, you don't -- to understand how the system
15 operates in the patent, you don't need to know security
16 and proofs, but to understand the science of how these
17 things are being developed and how they --

18 (Court reporter requested clarification.)

19 THE WITNESS: -- how they work together or fit
20 together, you can make use of security reductions and
21 proofs.

22 BY MR. KHAN:

23 Q. So in paragraph 10, you use the word "subject
24 matter," which is what I was questioning you about.

25 So is it not clear to you whether the word --

1 the phrase where I'm using "subject matter" as used in
2 your declaration, what that entails?

3 A. To me, entails the subject --

4 MR. HENRY: Objection. Objection. Substance
5 of the -- or the format of the question. I don't see
6 the word "subject matter" in paragraph 10.

7 MR. KHAN: I'll read the question of the
8 patent --

9 MR. HENRY: Oh, I'm sorry. I do see it. Can
10 you ask the question again, please?

11 MR. KHAN: Yeah. So Dr. Preneel, in his last
12 statement, had mentioned that it wasn't clear to him
13 what I meant when I was asking about subject matter
14 relevance, and I was indicating that I'm quoting his
15 paragraph 10 language that said, "I am a technical
16 expert in the subject matter areas relevant."

17 BY MR. KHAN:

18 Q. And so my question was, that term as used in
19 your declaration, is it not clear to you what that term
20 includes, hence the confusion in my question; or is -- I
21 guess I'm trying to understand why there's confusion
22 when that term is used in your declaration.

23 A. I'm not sure I fully understand what you're
24 asking. I mean, how I define "subject matter areas
25 relevant to this matter"? Is that -- you want me to

1 define this, or you want to define the scope of this?

2 Q. I'd like to understand what you're trying to
3 say here. I am trying to understand whether your
4 statement is saying -- when you're saying "subject
5 matter areas relevant to this matter," all right, what
6 are you trying to say to these -- the list that we've
7 been discussing, is this related -- is this related to
8 the specification for context? Is it related to the
9 claims?

10 I am asking you for clarity, and hence my last
11 questions were related to, is this required in the
12 claims or relevant to the claims or -- or subject matter
13 understanding. So that's why I was, you know, trying to
14 get a better sense of what your -- what you mean by this
15 particular sentence.

16 A. When I say "subject matter areas relevant to
17 this matter," okay, I mean this is all of the technical
18 and scientific tools you need to fully understand all of
19 the aspects of the technology studied in this patent,
20 which means not only the description and the scope of
21 the techniques, but also to fully understand the
22 security and weaknesses and shortcomings.

23 Now, if you specifically limit this to whether
24 a certain claim is valid or not or whether -- you need
25 to understand what the scope is of the claim in the

1 patent, I do think this is limited. I would say the
2 definition would be more limited and restricted to
3 secure execution environments and secure electronic
4 transactions in the first place --

5 (Court reporter requested clarification.)

6 THE WITNESS: -- execution environments and
7 secure electronic transactions in the first place, but
8 of course, also cryptographic hardware and software
9 because they are used in the claims, and then
10 cryptographic algorithms and protocols.

11 The cryptanalysis security reductions and
12 proofs, they are only there to understand security of
13 the schemes and to understand how valuable they would be
14 in a specific context. I hope that helps to clarify.

15 BY MR. KHAN:

16 Q. Thank you.

17 Going back to paragraph 8 of your declaration,
18 just two paragraphs up, would you let me know when
19 you --

20 A. Yes, I have it in front of me.

21 Q. Thank you.

22 You mention in paragraph 8 that, in forming
23 your opinions, you reviewed the '766 patent, the '480
24 patent, the respective file histories, the exhibits that
25 were submitted by the Petitioner; is that correct?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. That's correct.

2 Q. You also mention that you have relied upon
3 your education, experience, and knowledge of engineering
4 practices and principals in the cryptographic algorithm
5 industry; is that correct?

6 A. That's correct.

7 Q. In the last sentence on -- in paragraph 8, you
8 mention that, "I have also relied on publication
9 relevant to the technology in this matter"; is that
10 correct?

11 A. That's correct.

12 Q. What's the publication that you're referring
13 to in that sentence?

14 A. Well, I guess it should read "publications"
15 because there was, of course, a large cryptographic
16 literature on this topic, liter- -- on the topic of how
17 to implement secure execution environments.

18 Q. Which publications are those?

19 A. I should have to go look up the list. I mean,
20 I don't have the list in front of me. But, of course,
21 I've been working in this area very early on because I
22 was, for example, involved in secure smart cards. There
23 was quite some literature on secure smart cards, and I
24 can provide you details on this.

25 I've also -- this is, of course, in the period

1 after patent was filed, so more recently, I've been
2 working myself. So I was -- around 2000, I was involved
3 in TPM, initially called TPCA, Trusted Platform
4 Computing Alliance, which was later renamed to TPM,
5 Trusted Platform Module, and I was an international
6 advisor to this organization. And together with my PhD
7 student, I wrote publications about the security of
8 TPMs. These are trusted modules which are added to a PC
9 to -- and house their security.

10 And so more recently, I've also worked on
11 developing secure execution environments and the key
12 management in those environments. One example is the
13 literature on Sancus and Sancus 2.0, which is an
14 environment --

15 (Court reporter requested clarification.)

16 THE WITNESS: Sancus, S-A-N-C-U-S. Sancus is
17 a Latin word. It's a secure execution environment which
18 we designed about ten years ago.

19 So what I want to put out with the statement
20 is that I've been active as a researcher in this topic
21 since the late '80s, and that's how I've been keeping
22 up-to-date with the scientific literature on this, but
23 also with industry developments such as what happened in
24 the framework of TCPA and TPM.

25

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. So in relying -- in forming your opinions and
3 relying on these other publications, are there any of
4 these publications that you used to form your opinions
5 but did not cite in your declaration?

6 A. I don't think it's the case. I think I refer
7 here to publications are referred is that these
8 publications and this work we did provide me general
9 understanding of the field on what is possible and what
10 is not possible. But I don't think that this general
11 knowledge was literature to specifically cite to this in
12 this deposition -- or in this declaration.

13 (Court reporter requested clarification.)

14 THE WITNESS: I would say "literature," I
15 said.

16 THE REPORTER: "General literature," would
17 that be --

18 THE WITNESS: Yes.

19 THE REPORTER: Okay. Thank you.

20 BY MR. KHAN:

21 Q. So there's no position here in your
22 declaration that was -- that relied on evidence that you
23 did not cite to; is that --

24 A. In the publication -- can you please clarify
25 the question? Because I'm not sure I fully understand

1 it.

2 Q. My question was that there is -- is it correct
3 to say that there's no missing reference or citation in
4 your declaration that you perhaps may have used to
5 support to -- to develop your opinions here, but did not
6 bring to the record?

7 A. No, I don't think that it was necessary to add
8 citation literature also because most of the citations
9 are much more recent, but they do develop my general
10 understanding of what is happening because sometimes we
11 can learn things also in hindsight.

12 Q. Now, you've mentioned that you have a lot of
13 experience in this area. Does that include teaching
14 classes in this subject matter you mentioned in your
15 declaration?

16 A. Since the late '90s, I've been teaching
17 classes on applied cryptography and network security,
18 but I've also been providing specific industry trainings
19 on secure implementations and on hardware security,
20 which typically involves things like secure execution
21 environments.

22 Q. In the past five years, how many such classes
23 have you taught?

24 A. So applied cryptography and network security,
25 so the general cryptography course I've been teaching

1 every year plus in two classes, and then I think, like,
2 just for industry I would say on this topic two to
3 three.

4 Q. And how big are these classes?

5 A. My applied cryptography and network security
6 course has 80 students, and I also have a condensed
7 version of this course with about 5 to 10 students. On
8 my teaching to specific industry is typically group of
9 size 8 to 10.

10 Q. And the curriculum or the material that's
11 covered in these classes, does that include hardware and
12 software or is it just for one of the two?

13 A. So the dedicated courses do include both
14 hardware and software.

15 Q. You mentioned earlier, I think, and also in
16 the context of paragraph 10 again also, you mentioned
17 secure execution environments.

18 Why is that -- why is that so relevant or
19 important in the '766 patent?

20 A. Because the '766 patents actually in it claims
21 it has a memory device in the electronic device storing
22 of the private key in a secure area of the electronic
23 device, and it also has authentication software in a
24 secure area inaccessible to the operating system. So
25 it's clear that the scope of the patent and of this

1 claim is to have a secure execution of an electronic
2 transaction inside a secure environment in a protected
3 memory.

4 Q. How does secure environment -- what is
5 required for a secure environment to be in place in
6 these computer systems as described in the '766 patent?

7 A. Well, we can start with Claim 1. You have --
8 of course, in this case you have an electronic device.
9 It has an operating system. And on top of that, there
10 is user applications, and then secondly, there is a
11 secure operating environment independent of the
12 operating system. So it's very important that the
13 operating system and there's also the user applications
14 cannot access this secure environment because the user
15 environment is easily compromised and, in general for
16 these transactions, the users are not trusted.

17 So you want to get a separation with the
18 secure electronic environment on the one hand where you
19 do the --

20 (Court reporter requested clarification.)

21 THE WITNESS: -- to do the computation, so to
22 execute the authentication software, and on the other
23 hand, the operating system and the user applications.

24 And, of course, to create a secure
25 environment, you then need a secure memory or memory

1 location which is, again, not accessible to the
2 operating system. And the secure area needs a private
3 key for computing the secure transaction and also needs
4 software, again, to compute a secure transaction.

5 And then the matter to authenticate this
6 software, these are the elements described in the '766
7 patents.

8 BY MR. KHAN:

9 Q. So my question was a little bit different.
10 I'm going to repeat it.

11 My question was, what is required for a secure
12 execution environment? I understand you're telling me
13 what Claim 1 is saying, but I'm asking you, you know,
14 more generally, what's required for a secure execution
15 environment?

16 A. In general, what you want is -- I think that
17 there is a separation between, on the one hand, the user
18 side and, on the other hand, typically also the
19 operating system and, on the other hand, the environment
20 itself. So it is not possible for user software or for
21 compromised user software or for operating system
22 software or compromised operating system software to
23 access the secure environment.

24 Q. So how do the systems operating in these
25 secure execution environments create that -- that

1 ability to sort of make the operating system -- that
2 division there you're talking about, the
3 inaccessibility, how does the secure execution
4 environment do that?

5 A. Well, typically you have a layer below the
6 operating system that separates the operating system
7 from some other piece of software, for example, the
8 console, or you try to fully implement this in hardware.
9 And so what you try to do is try separate the memory and
10 the code from a secure environment from that from the
11 regular environment.

12 Q. So is the console typically between the
13 operating system and some other layer? Is that what
14 you're saying?

15 A. The console would sit at the same level as the
16 operating system, and there is a layer below that
17 actually separates those two. And you can see the
18 console as a simplified operating system that's only
19 there to run the secure environment, just as the
20 operating system is there to run the user applications.

21 Q. I see.

22 So -- so the console is like an operating
23 system except it's not used to run the user applications
24 that are receiving user input; is that correct?

25 A. It's typically much more restricted in

THE SULLIVAN GROUP OF COURT REPORTERS

1 functionality, which makes it also easier to make it
2 secure.

3 Q. I see.

4 So is it possible to have multiple operating
5 systems in a computer?

6 A. Yes, it is.

7 Q. And one of those could act like the console?

8 A. Yes. It would be called -- the operating
9 system would be called a console then.

10 Q. I see.

11 Turning to paragraph 20 of your declaration.
12 Can you let me know when you get there?

13 A. Yes, I have that.

14 Q. So I'll read it for the record. Paragraph 20
15 states, "I understand that the board may not institute
16 post-grant review unless the petition 'information
17 presented in the petition filed under Section 321, if
18 such information is not rebutted, would demonstrate that
19 it is more likely than not that at least one of the
20 claims challenged in the petition is unpatentable.'"
21 End quotes there.

22 Is that a correct reading of paragraph 20?

23 A. That's correct.

24 Q. The first sentence. Yeah. Okay.

25 Did you apply this standard in --

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Yes, I did.

2 Q. Okay. What does the -- in paragraph 22, two
3 paragraphs down, you mention that the, "Patent claims in
4 an IPR are given their broadest reasonable
5 interpretation ('BRI')"; is that correct?

6 A. That's correct. Yes.

7 Q. Did you apply the BRI standard to review the
8 '766 patent?

9 A. Yes, I did.

10 Q. In paragraph 20, you mention post-grant
11 review, and in paragraph 22 you mention IPR.

12 Can you tell me what the difference between a
13 PGR and IPR is?

14 A. So I see two times in 20 and 21 post-grant
15 review. Maybe I misunderstood your question, but...

16 Q. So I'll repeat my question. In paragraph 20,
17 you mention "post-grant review." In paragraph 22, you
18 say "patent claims in an IPR."

19 My question is, what's the difference between
20 a PGR and an IPR?

21 A. It must be a typo because the version I have
22 in front of me says "PGR."

23 Q. I'm sorry. What does it say?

24 A. This must be a problem that occurred because,
25 in fact, the version I have in front of me says "patent

THE SULLIVAN GROUP OF COURT REPORTERS

1 claims in a PGR," the correct statement. So there may
2 have been some editing error in both.

3 Q. Okay.

4 A. So the correct version is PGR as far as I
5 understand.

6 Q. So I will maybe -- I'd like to make sure we
7 have the same copy. So what I can do is I can drop the
8 file for the exhibit into the chat and then --

9 A. I have the file in front of me. I mean, I
10 have the two files in front of me, the one --

11 Q. My concern is --

12 A. Yes, I know it says IPR, but it should be PGR.

13 Q. My concern is that the version that you're
14 looking at is not the same one that's filed.

15 A. Okay.

16 Q. And I'd like to make sure that as we move
17 forward we're looking at the same document so that
18 they're not -- there is no confusion.

19 So I am going to send you the filed version,
20 or if your counsel would like to send you the filed
21 version, that is also okay. I would prefer to send it
22 to you, but if -- unless your counsel has any objection
23 to that --

24 MR. HENRY: No, I'd prefer that you do it.

25 MR. KHAN: Okay. Great. Give me one second,

THE SULLIVAN GROUP OF COURT REPORTERS

1 please. I'll send it to you.

2 BY MR. KHAN:

3 Q. Dr. Preneel, please let me know when you have
4 the file open.

5 A. I have it open in front of me. I also have
6 the printout of it next to my own version which I have
7 my notes on. That's why I was using that version.

8 Q. Okay. So moving -- moving forward, I think
9 I'll be referring to the filed document, right --

10 A. Yes.

11 Q. -- and asking you questions accordingly. I
12 don't know the contents of whatever else you're looking
13 at, so I'd rather not have you look there.

14 MR. KHAN: So -- but, Ms. Houston, do you have
15 a copy -- were you able to download a copy too?

16 COURT REPORTER: I was. Thank you so much.

17 MR. KHAN: Great.

18 BY MR. KHAN:

19 Q. Okay. Up until -- I'd just like to confirm,
20 up until now, the questions I've been asking you, were
21 they consistent with the copy that you had seen?

22 A. Yes, they were.

23 Q. And your opinion is consistent with the file
24 that I just sent you, Exhibit 2009, a copy of --

25 A. Yes, it is. Yes.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Okay. So I'm going to ask -- pick up from
2 where we just were.

3 In the Exhibit 2009 that we are looking at, in
4 paragraph 20, is it correct that your paragraph 20
5 states, "I understand that the board may not institute
6 post-grant review ('PGR') unless the petition" -- and
7 I'll stop there.

8 Is that correct?

9 A. That's correct, yes.

10 Q. In paragraph 22, you state that the, "Patent
11 claims in an IPR are given their broadest reasonable
12 interpretation ('BRI')."

13 Is that correct?

14 A. That's correct, yes.

15 Q. And you use the BRI standard for your
16 opinions; is that correct?

17 A. That's correct, yes.

18 Q. Can you tell me what the difference is between
19 a PGR and an IPR?

20 A. Well, the post-grant review was the first
21 phase in which there was a petition and there was a
22 request to go to a IPR procedure. And my understanding
23 is we're now in the IPR procedure. So first there was
24 an indication that there's -- it's more likely than not
25 that at least one of the claims challenged in the

1 petition is unpatentable, and then this question is
2 actually sorted out in the IPR procedure. That's my
3 understanding.

4 Q. And so is it your understanding that first we
5 are in a PGR and then we move to an IPR?

6 A. Yes.

7 Q. And we didn't discuss it at the outset, but
8 make it clear now. As you know, we have a second
9 deposition scheduled for Friday. And just to make it --
10 I guess the lines a little bit -- well, just to
11 facilitate our discussion, what I was planning on doing
12 is questioning you on the '766 patent today and the '480
13 patent on Friday. Does that sound okay to you?

14 A. That's fine, yes.

15 Q. Okay. So my questions today will be limited
16 to your '766 declaration. Is that okay?

17 A. That's fine.

18 Q. Great.

19 In paragraph 22, you mention that, and I'll
20 quote, "The BRI of the claim terms is understood from
21 the perspective of a person of ordinary skill in the
22 art."

23 Is that correct?

24 A. That's correct.

25 Q. Who is a person of ordinary skill in the art?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I think that somebody -- I don't remember
2 whether my -- my working definition, but it's somebody
3 who had a basic knowledge of a specific subject matter
4 of the patent. This typically is somebody, say, with a
5 bachelor degree with a few years of experience or
6 somebody with a master degree or PhD degree, I think in
7 this case, who would understand the subject matter
8 necessary to -- as we discussed earlier, to apply and
9 understand the patent.

10 Q. So is it your position that a person of
11 ordinary skill in the art is someone who has a
12 bachelor's or master's or PhD degree in the subject
13 matter areas that you noted in paragraph 10, which was
14 cryptographic algorithms and protocols, cryptanalysis --

15 (Court reporter requested clarification.)

16 MR. KHAN: I'm really sorry.

17 THE REPORTER: That's okay.

18 BY MR. KHAN:

19 Q. So I'll continue. Maybe I'll repeat my
20 question.

21 So is it your opinion that a person of
22 ordinary skill in the art, as you note in paragraph 22,
23 is a person who has a bachelor's or a master's or a PhD
24 degree in the subject matter areas that you've listed in
25 paragraph 10, which include "the design and evaluation

1 of cryptographic algorithms and protocols, including
2 cryptanalysis, security reductions and proofs,
3 cryptographic hardware and software, secure execution
4 environments, and secure electronic transactions"?

5 A. First, I don't think that a bachelor degree in
6 most cases is sufficient because it's quite advanced
7 matter.

8 Second, these degrees, of course, don't exist.
9 I mean, you have degrees of computer science or
10 electrical engineering where you have -- typically to
11 understand these matters, you get basic notions of
12 computer science and computer architecture, and then
13 hopefully or ideally such a person should also have at
14 least some courses on computer security or cybersecurity
15 and cryptography.

16 Q. So is it your position that a person of
17 ordinary skill in the art would have a bachelor's,
18 master's, or PhD degree in electrical engineering
19 focused on the topics you just mentioned? Is that
20 correct?

21 A. I think you need to have a general
22 understanding of either computer science or electrical
23 engineering courses. Typically -- CS courses typically
24 have some courses on computer architecture which you
25 would need to understand the hardware, and the EE

1 courses typically have some computer science subject
2 matters, so that would be the general degree, so to have
3 a general understanding of what's happening or how
4 computers operate and how the systems work. And having
5 it would -- I would assume that somebody has also some
6 course in cybersecurity or applied cryptography.

7 Q. Does --

8 A. Then in this moment to be an expert in
9 cryptanalysis or -- I don't expect this person to be an
10 expert for the cryptanalysis or security proofs but to
11 have a general understanding of what these things are,
12 what the security proof is, or what these notions are at
13 a very high level. And I think I also already repeated
14 that I don't believe that a bachelor degree is
15 sufficient to be -- in this matter, a person of ordinary
16 skill in the art would need to have at least several
17 years of industry experience, given the scope of most
18 bachelor programs.

19 Q. So is it correct to say that you think at
20 least a master's or a PhD degree with work experience
21 is -- is what is needed to be a person of ordinary skill
22 in the art?

23 A. I don't think I said that. I think I said a
24 bachelor degree with a few years of experience or a
25 master degree or a PhD degree because during master or

THE SULLIVAN GROUP OF COURT REPORTERS

1 PhD degree, this experience can also be acquired.

2 Q. Do you think having a doctorate degree is what
3 a person of ordinary skill in the art would have?

4 A. No. That's not necessary.

5 Q. But it's possible?

6 A. They could have this, yes, but it's not
7 essential to have a doctor's degree.

8 Q. Which year did you get your PhD in?

9 A. 1993.

10 Q. So is it correct to say it's been about
11 29 years since you got your PhD?

12 A. That's correct.

13 Q. So how do you understand the perspective of a
14 person of ordinary skill in the art minus -- I'm sorry,
15 let me scratch that, please.

16 You're an expert in this area as you have
17 noted in your declaration according to you. How do you
18 understand the perspective of someone who just has
19 ordinary skill in the art, given that you are an expert,
20 what a person of ordinary skill in the art thinks? How
21 would you understand that?

22 A. Well, I work on a daily basis with some of
23 those people because I do also teach a second year
24 bachelor course, so I am very well aware of what
25 bachelor students know and do not understand. I also

THE SULLIVAN GROUP OF COURT REPORTERS

1 teach at first and second year master level, where they
2 are slightly more advanced students. I think every year
3 I supervise about five master thesis, so these are
4 students who are at the end of their master and you see
5 how they become more mature and what they understand
6 about these kind of topics and how they develop their
7 skills.

8 I -- on a regular basis, I consult for
9 industry, and very often the people I deal with there
10 are not PhDs but people with technical experience,
11 sometimes very experienced people, sometimes more junior
12 people, and we discuss technical matters exactly on
13 these kind of topics. So I'm not sitting in an ivory
14 tower and I'm just talking to experts. In fact, I
15 interact and train people at every age of experience,
16 and I interact a lot with people in the industry as
17 well.

18 Q. So you mention in your answer, if I can
19 repeat -- please correct me if I'm wrong here. You
20 mention that, in part -- you can understand the
21 perspective of a POSITA, in part, at least because you
22 have undergraduate students with bachelor's degrees; is
23 that correct?

24 A. That's correct, yes.

25 Q. Didn't you mention also earlier that having a

THE SULLIVAN GROUP OF COURT REPORTERS

1 bachelor degree alone is not enough?

2 A. I mentioned that, but I just -- I understand
3 what is still needed to go beyond that. So I think I
4 understand what people understand and know at specific
5 level of experience in their training. And so, yes,
6 based on my experience with these students, I can
7 confirm that that would not be sufficient even after
8 completion of their bachelor degree.

9 Q. So does that mean your interaction with
10 bachelor students does not inform the perspective of a
11 person of ordinary skill in the art?

12 A. I respectfully disagree with this. It does
13 inform me because it shows what -- that they are not
14 there at this young level, so it actually also helps to
15 understand what is needed because you see what is
16 actually missing.

17 Q. So by talking to your bachelor students, you
18 understand what they don't know?

19 A. Exactly.

20 Q. Have you had discussions with them about what
21 they don't know?

22 A. I do, of course.

23 Q. And does that include the subject matter of
24 the '766 patent?

25 A. We tend not to discuss patents, but we do

1 discuss application, in this case, of discrete
2 [phonetic] mathematics, and we understand what the
3 limited understanding is of systems and complexity of
4 things fitting together, so we do understand how they
5 can apply scientific results to real-life systems and
6 what their concerns are, what their difficulties are.

7 Q. Have you discussed the '766 patent with your
8 students or your colleagues?

9 A. No, I have not.

10 Q. So your thoughts on the perspective of a
11 POSITA are not based on conversations with people you
12 consider POSITAs; is that correct?

13 A. That's not correct because, as I mentioned
14 earlier, I worked with a PC student and we wrote
15 scientific articles on the security of TPMs, and these
16 are trusted platform modules, and they are very similar
17 ideas. They use secure execution environments for their
18 cryptographic keys, and so we actually are looking at
19 how to -- a better security of these components. And so
20 at that moment, this person was somebody who had a
21 master's degree working towards his PhD degree, so I
22 would consider this person at that stage to be a POSITA.

23 So I do have -- worked with people at the
24 POSITA level on specific -- unrelated to the specific
25 patent but on related problems, mainly secure execution

THE SULLIVAN GROUP OF COURT REPORTERS

1 environments and cryptographic transactions, secure
2 transactions.

3 BY MR. KHAN:

4 Q. When was -- this PhD thesis that you're
5 referring to, what date was that PhD thesis?

6 A. I would have to look it up, but I would say
7 work was probably done between 2004 and 2008 or so,
8 2009, something like this.

9 Q. Does a POSITA's understanding have any timing
10 elements to it?

11 A. Well, I guess POSITA means state of the art,
12 so of course that evolves with time, of course.

13 Q. And what time would that be?

14 A. I guess a time when the invention was filed.

15 Q. So when it comes to the '776 patent, the
16 filing date of the '766 patent, which would be June 14,
17 2004; is that correct?

18 A. That's correct.

19 Q. And the '480 patent is the same family that
20 had a filing date, I think, in -- well, we can get to
21 that when we talk about the '480. I don't want to mix
22 it.

23 A. Okay.

24 MR. KHAN: Okay. So we've been going for
25 about an hour. If you think we can maybe take a five-,

THE SULLIVAN GROUP OF COURT REPORTERS

1 ten-minute break. Does that work for you?

2 THE WITNESS: That's fine for me.

3 MR. KHAN: Mr. Henry, does that work for you?

4 MR. HENRY: Yes.

5 MR. KHAN: Great. So maybe we can reconvene
6 in ten minutes.

7 Ms. Houston, does that work?

8 COURT REPORTER: Of course. Thank you.

9 (Recess: 9:12 a.m. to 9:24 a.m.)

10 BY MR. KHAN:

11 Q. Dr. Preneel, during the break, did you
12 communicate with your patent owner's counsel?

13 A. No, I did not.

14 Q. Can I ask you to turn to paragraph 7 of your
15 declaration, please?

16 A. Yes.

17 Q. In paragraph 7, you state, "Al-Salqan and
18 Searle do not overcome the deficiencies described in the
19 patent owner's response relating to the combination of
20 Ellison and Muir."

21 Is that correct?

22 A. That's correct.

23 Q. Did you read or review the patent owner
24 response?

25 A. I did.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. So did you read it before or after writing
2 your declaration?

3 A. I read it before writing my declaration.

4 Q. Do you agree with all of the contents of the
5 patent owner response?

6 A. Obviously I don't agree with all of the
7 contents because that's what I try to make here in my
8 declaration.

9 Q. So you --

10 A. Maybe I misunderstood your question. Excuse
11 me. The patent owner response or did you say the
12 petitioner's response? Sorry.

13 Q. I said the patent owner response.

14 A. Okay. I agree, of course, with what is in
15 there. Excuse me. I did read that correction before I
16 wrote my deposition [sic], and I do agree with what is
17 in there.

18 Q. And did you write the declaration?

19 A. Yes, I wrote the declaration.

20 Q. Did you write any part of the patent owner
21 response?

22 A. I did not.

23 Q. Did you -- let me ask you -- I'm sorry. One
24 second, please.

25 In writing your declaration, did you discuss

THE SULLIVAN GROUP OF COURT REPORTERS

1 the contents of your declaration with counsel?

2 A. Yes, I did.

3 Q. Did you attempt to make sure that your
4 comments and arguments were consistent or the same as
5 the patent owner response?

6 A. There were some consultations, and I did my
7 best to write on my technical opinions, but in the end
8 if there would be deviations -- which I haven't seen --
9 that would not be deliberate in any case.

10 Q. So is it correct to say that if there is any
11 difference, it is not your intention to make it
12 different? Is that correct?

13 A. That's correct, yes.

14 Q. Do you have --

15 (Court reporter requested clarification.)

16 BY MR. KHAN:

17 Q. Do you have a copy of the patent owner
18 response with you, Dr. Preneel?

19 A. I don't have it printed, I believe.

20 Q. Okay. Let me --

21 A. If you show it -- it would be nice if it could
22 be projected or if you could just mail it to me so I'm
23 sure I have the right version.

24 Q. Yes, I'll drop it in the chat box like last
25 time.

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Okay.

2 Q. I'm sorry. I'm sorry. Please disregard that
3 copy.

4 Okay. I'm going to share my screen with you,
5 if that's okay.

6 A. That is fine.

7 Q. Okay. Can you see my screen?

8 A. Yes, I can.

9 Q. Okay. I have shown on my screen the patent
10 owner response.

11 Can you confirm that this is the patent
12 owner's response?

13 A. That's correct, yes.

14 Q. I'm turning to page 24, and page 24, the last
15 paragraph here reads, "The usage protector 250 are
16 loaded into the execution space by processor nub
17 loader 52."

18 There's some citations there. And then it
19 states, "These loaded modules are stored in mass storage
20 device 170 which can be a CD-ROM 172, floppy diskettes
21 174, and a hard drive 176."

22 There's a cite to Exhibit 1006 and then a cite
23 to Exhibit 2009, paragraph 54. Is that correct?

24 A. That's correct. Yes.

25 Q. The last citation there, Exhibit 2009,

THE SULLIVAN GROUP OF COURT REPORTERS

1 paragraph 54, do you agree that that is a citation to
2 your declaration?

3 A. I don't know the number by hand of the
4 exhibit. If you confirm that my declaration is 2009,
5 then I confirmed it, yes.

6 Q. Okay. Then can you turn to paragraph 54 of
7 your declaration, please.

8 I'll stop sharing right now.

9 Could you read paragraph 54 for me, please.

10 A. "The goal of usage protector 250 is" --

11 (Court reporter requested clarification.)

12 THE WITNESS: "The goal of usage protector 250
13 is to protect the secure processing environment itself
14 and not the transactions."

15 BY MR. KHAN:

16 Q. So, Dr. Preneel, paragraph 54 speaks to the
17 goal of the usage protector, correct?

18 A. That's correct.

19 Q. And there are no citations in this paragraph,
20 correct?

21 A. That's correct.

22 Q. The paragraph includes no statement about a
23 storage device, correct?

24 A. That's correct.

25 Q. The paragraph includes no description of

1 loading the usage protector, correct?

2 A. That's correct.

3 Q. And paragraphs 50 to 72 of your declaration do
4 not include a single citation; is that correct?

5 A. That's correct.

6 Q. Okay. So in -- I'm sorry. I'll pause there.

7 Now I'd like to ask you to open up a copy of
8 the '766 patent.

9 A. Yes, I have it in front of me.

10 Q. Thank you.

11 In paragraph 41 of your declaration, you state
12 that, "The '766 patent claims a novel, method, and
13 system for performing an electronic transaction or
14 electronic verification or identification without
15 requiring additional hardware."

16 Is that correct?

17 A. That's correct.

18 Q. It also states that in your opinion, "The
19 interventions claimed in the '766 patent represented
20 significant steps forward in electronic transaction
21 technology and verification of legitimate access to, or
22 use of digital data."

23 Is that correct?

24 A. That's correct.

25 Q. What are the -- can you explain what the '766

THE SULLIVAN GROUP OF COURT REPORTERS

1 patent is referring to when they are saying "without
2 requiring additional hardware"?

3 A. There was really two approaches to make secure
4 transactions processors, and one is providing additional
5 hardware to secure keys -- to secure potentially the
6 software to complete the transaction, and to isolate
7 this, but one can also do this with existing methods.
8 For example, by modifying the BIOS and by only --
9 software-only methods. And so I think this particular
10 paragraph refers to the fact that it can also be done
11 without additional hardware.

12 Q. And what hardware is that?

13 A. You mean which -- the one which is not added
14 or the --

15 Q. Yes. Which hardware is not added?

16 A. There will not -- for example, not add
17 hardware circuits to, for example, separate memory. Or
18 you would not have special additional hardware to store
19 cryptographic keys or to perform cryptographic
20 computations. So if you go back 20 years ago, people
21 weren't particularly thinking of having the smart card,
22 and they would issue it by a bank, and during the
23 transaction it's like a smart card --

24 (Court reporter requested clarification.)

25 THE WITNESS: So 20 years ago, you would have

1 been thinking of securing transactions by performing
2 them inside a smart card provided by a bank, and a
3 secure environment would then be the smart card, and the
4 smart card would be the additional hardware.

5 BY MR. KHAN:

6 Q. You mentioned that using potential software
7 secure -- sorry, you could use potential software to
8 secure a transaction.

9 Did I repeat that correctly?

10 A. That's correct, yes.

11 Q. What kind of software is typically used to
12 secure the transaction? And this is, again, you know,
13 going back where we were talking about, I think, when
14 the filing date or -- you know, at the filing date or
15 around that time for the '766 patent, what was the
16 software that would be used to secure transactions?

17 A. Well, at the time transactions were just
18 carried out in browsers. There was no additional
19 software or hardware provided. People just entered
20 transaction data, including payment data, in a
21 browser -- on a regular browser on a regular computer
22 using a regular operating system on regular hardware.
23 And, of course, this exposes the credit card
24 information, also the transaction itself to attacks on
25 either the operating system or on the browser or the

1 user application.

2 Q. So at that time there were no cryptographic
3 keys?

4 A. Cryptographic keys were used inside the
5 browser. So already in 1993, '94, the SSL protocol was
6 created, which later became TLS protocol, and that
7 protocol provided a secure channel between a browser on
8 the one hand and a server at the merchant on the other.
9 For the secure channel, cryptographic keys were used,
10 but there was no cryptography used to protect the
11 transaction itself. It was just entered through the
12 secure channel and transferred to the other side.

13 Q. So at that time were digital signatures used?

14 A. It depends on the context and the setting.
15 Very specifically, digital signatures, at least of the
16 definition which is also used in this patent, which also
17 includes what cryptographers call MAC algorithms or
18 symmetric key signatures, they were in use already since
19 the '80s in the banking sector.

20 Digital signatures were also in use using
21 public key technology in the credit card sector, you
22 have read specifications for which I was a reviewer in
23 the early '90s. This technology was, at that time,
24 rolled out in Europe late '90s but not yet in the US.
25 It came much later in the US, but in Europe, it was

THE SULLIVAN GROUP OF COURT REPORTERS

1 available. Digital signatures were also used, for
2 example, in -- I would say not in the US but several
3 countries in Europe including Belgium --

4 (Court reporter requested clarification.)

5 THE WITNESS: Belgium, that's the country
6 where I live -- Belgium and Estonia were issued digital
7 or electronic identity cards, and you could compute with
8 those digital signatures. So the answer is, yes,
9 signatures were used, but not for Internet transactions.

10 BY MR. KHAN:

11 Q. I see.

12 So as of 2003, you're saying digital
13 signatures were used but maybe for other applications,
14 not for Internet applications; is that correct?

15 A. They were used for electronic transactions as
16 described in the patent but not when implemented on the
17 Internet.

18 Q. I see.

19 And the digital signatures that are used, are
20 they -- as of 2003, are they also -- are they used --
21 are they generated using a private key or a public key
22 or at that -- 2003, how were the digital signatures
23 generated?

24 A. As I mentioned in my previous answer, there is
25 two options. One is based on symmetric cryptography,

1 which cryptographers call MAC algorithms, or message
2 authentication codes, and in that case the signer and
3 the verifier or sender and recipient share a secret key.
4 And that is the model used in most banking cards,
5 typically debit cards, and it's still also used in a
6 number of debit cards, credit card transactions today.

7 But in some other settings, in typically
8 credit card payments following the EMV specifications --
9 and those specifications were created in '93, '94, '95,
10 so first half of the '90s -- their digital signatures
11 were used that used a private key to sign a transaction
12 and a public key to verify the transaction.

13 And this was rolled out by EMV under the term
14 "combined data authentication." Combined because you
15 would use both a digital signature based on asymmetric
16 keys and a second digital signature based on a MAC
17 algorithm with shared keys. So at the time of the
18 invention, both technologies were in use for financial
19 transactions.

20 Q. And at that time in 2003, did they --
21 specifically June 2003, did they have architecture that
22 would be able to secure the private key and allow for
23 secure transactions to occur?

24 A. I think definitely there were several banks
25 and this is -- I was aware of this, but most of those

THE SULLIVAN GROUP OF COURT REPORTERS

1 things were proprietary protocols. For example, in
2 Europe, there were several banks that actually used
3 software-based solutions to secure digital banking with
4 private keys stored somewhere on the user device,
5 typically encrypted under a user password.

6 Q. And in 2003, in June 2003, how would they --
7 so you mentioned that there were several protocols.

8 How would they secure the private key? Like
9 what would these protocols do?

10 A. For the majority of transactions, the private
11 key was stored in a smart card issued by the bank or the
12 financial institution, and this was a problem because,
13 of course, a smart card -- it's hard to connect a smart
14 card with a PC platform. There were banking solutions
15 that provided this but not for retail banking, so there
16 were wholesale banking applications where you could use
17 a smart card to authorize your transactions. But this
18 was deemed to be too complex and too expensive to
19 support for retail applications. So this was used for
20 business-to-business scenario.

21 For retail applications, so for consumer
22 transactions, this private key was just stored somewhere
23 on the device or in the browser encrypted using very
24 often the password of the user.

25 Q. As you said, the private key would be in a --

1 stored in an encrypted form in the memory.

2 A. But as a very weak encryption because it was
3 the password of the user.

4 Q. I see.

5 A. And sometimes it was not encrypted at all.
6 There were applications where it was stored in Clear.

7 Q. And how would the private key be -- scratch
8 that.

9 You mentioned that the private key would be
10 encrypted perhaps using the user's password, login
11 information; is that correct?

12 A. That's correct.

13 Q. When it was -- when the private key was stored
14 in memory and in encrypted format, was it protected in
15 any way or was it left vulnerable for anyone to take?

16 A. It was not protected in any way. So both the
17 encryption process itself and the outcome of the crypto
18 private key was available in clear. And, again, I'm
19 referring here to the scenario on a PC, not the scenario
20 where a smart card is used.

21 Q. So when the encryption or decryption was
22 performed, where -- where would that be performed?

23 A. Just on the regular processor in normal
24 software, and so both the operating system and the user
25 software had access to this.

1 Q. Would that be in a -- I guess, would that be
2 in a secure area where they did --

3 A. No --

4 Q. -- perform the encryption or the decryption?

5 A. No, it was done in what we call insecure
6 memory.

7 Q. I see.

8 Now, in paragraph -- going back to
9 paragraph 31, you -- the second statement in that
10 paragraph, you also mentioned that the '766 patent
11 represented some "significant steps forward."

12 What are these significant steps forward?

13 A. The step forward is the idea of creating two
14 environments, on the one hand -- I'm now referring here
15 to Figure 3, the operating system. And then the secure
16 environment run by the console, and there was a secure
17 area, and this area has secure storage of the key but
18 also secure storage of authentication software. And in
19 addition, the key would be encrypted and also decrypted
20 all in a secure environment. So even if the user
21 application, say, the browser or the operating system
22 would be compromised, it would not be possible to get
23 access to the keys or to manipulate authentication
24 software in the secure environment. So it was like
25 creating a smart card inside the computer.

1 Q. What prevents the operating system from
2 accessing the secure area?

3 A. The BIOS prevents this because the operating
4 system has to use the BIOS, and the BIOS, you cannot
5 just use it. You have to go to an API call, so it's
6 called the vector table, so it's a regulated interface,
7 and this BIOS would deny access to certain places in
8 memory to the operating system.

9 Q. Can you explain -- can you indicate what a
10 BIOS -- what it stands for and what its function is?

11 A. A BIOS is the basic input/output system. It's
12 active when the system starts up, when the system boots,
13 as we say with technical terms. So when the computer
14 starts up, the first program run will be the BIOS, and
15 the BIOS will prepare the computer for working.

16 And then secondly, during operation of the
17 system, the BIOS will mediate access to memory and to
18 other devices such as printers or network ports on the
19 computer. So the operating system, it wants to use
20 memory or wants to use certain ports, it has to go
21 through the BIOS, and the BIOS can give access or -- in
22 the example of the design in Figure 3 -- also, in
23 certain cases, deny access.

24 Q. So is it correct to say that the BIOS can
25 permit access or restrict access to the secure area?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. That's correct, yes.

2 Q. Thereby rendering the secure area inaccessible
3 to the operating system; is that correct?

4 A. That's correct.

5 Q. Can the BIOS be split into different areas?

6 A. It's possible to make the BIOS more complex
7 and to have more complex designs, and as I mentioned,
8 the BIOS has already two functions, the startup function
9 and the operating function. So in practice, yes, it is
10 possible to do this. But that depends, of course, on
11 the design of the system, whether it's done or not.

12 Q. What about in Figure 3 of the '766 patent, is
13 that -- is that just one BIOS, or is it a BIOS that has
14 different parts?

15 A. That's one BIOS, but in this particular
16 example, the BIOS may contain also an encryption key
17 that can be used in the secure operation of -- secure
18 operation environments.

19 Q. So it's one BIOS -- so if I understood you
20 correctly, it -- in Figure 3 of the '766 patent, there's
21 one BIOS, not divided, by --

22 A. That's correct.

23 Q. Okay. It includes an encryption key 46?

24 A. Yes.

25 Q. Can you turn to column 6, line 62, of the

1 patent.

2 Is it correct -- I'll read lines 61 to 62.

3 Is it correct to say that lines 61 and 62
4 read, "The encoded authentication table is stored in a
5 secure part of the BIOS"?

6 A. Yes.

7 Q. So is there an unsecured part of the BIOS?

8 A. Well, I think in this particular sentence,
9 what is meant by "secure part" is part that cannot be
10 read by the operating system. So "secure" is here
11 defined as the operating system cannot read or write
12 this. And BIOS is typically ROM, so it can't be
13 rewritten. But other parts, of course, can be read by
14 the operating system because it's needed to boot the
15 system or to perform certain actions.

16 Q. So is it -- is it accurate to say that the
17 BIOS can include a secure part and an insecure part, and
18 the insecure part is the one that communicates with the
19 operating system 48?

20 A. I think it's a bit more complex. I think
21 there is -- the BIOS consists of multiple pieces of
22 software, and part of it regulates the traffic, right,
23 and then it may give you access to certain part of the
24 BIOS or certain part of the system, and the other parts
25 implement a specific access.

1 Q. So more specifically when you say that it --
2 there are certain parts that give you access to certain
3 parts of the system and other parts that implement a
4 specific access, could you be a little more precise in
5 that? I'm not sure which part is giving access to what.
6 So if you could explain that to me, that would be --

7 A. Well, the core -- the core is that the
8 operating system will ask for access during operation of
9 the system. And then access will be implemented, which
10 means, for example, a connection will be set up with the
11 printer if the BIOS allows this or with the network or
12 with part of the memory, or the BIOS may say, no, you
13 cannot access this or this function is not available to
14 you. So there is code needed to implement the access,
15 and there is code needed to regulate the access in the
16 first place.

17 Q. So when the patent says there is a "secure
18 part of the BIOS," are they referring to just code,
19 that's the secure part of the BIOS? What are they
20 referring to when they say "secure part of the BIOS"?

21 A. Obviously it's data which cannot be read.
22 That secure part is data which cannot be read by the
23 operating system. The operating system asks to read it,
24 it will be denied. That's why we call it secure BIOS.

25 Q. So is that data being handled by a secure

1 processor or stored in a secure memory? What -- what
2 makes that secure part of the BIOS?

3 A. There is part of -- if the operating system
4 wants to read it, it will not get permission to do this.
5 That's why we call it secure part of the BIOS.

6 Q. So I'm asking about which part is secure,
7 which part's not secure, and your answer has been
8 whether the BIOS gives permission or not.

9 So I'm going to ask again. Which part of the
10 BIOS is secure? Which part is insecure? Not whether
11 one part gives permission or not. I'm trying to
12 understand when the patent -- '766 patent says "the
13 secure part of the BIOS," which part of the BIOS does
14 that include?

15 A. I think, Counselor, that the answer is as I
16 gave before. Secure part is the part which cannot be
17 read by the operating system, so there is part of the
18 BIOS that denies access to it where the operating system
19 has no read access.

20 Q. And what components form that secure part?

21 A. That part of the BIOS that decides about
22 access.

23 Q. So my question was, what components form the
24 secure part?

25 A. So would you mean what is -- maybe to -- to

THE SULLIVAN GROUP OF COURT REPORTERS

1 make sure I understand the question, what are the
2 components of the secure part of the BIOS; is that the
3 question?

4 Q. Yes.

5 A. What is in there? What comes in the secure
6 part? So there can be cryptographic keys, there can be
7 data for authentication of transactions, and also it
8 could be -- authentication software could also be stored
9 in there.

10 (Court reporter requested clarification.)

11 THE WITNESS: Authentication software.

12 BY MR. KHAN:

13 Q. But in Figure 3, isn't it the case that the
14 authentication software is in the secure area 62?

15 A. Yes. But it could also be stored in the BIOS.

16 Q. So in the BIOS in Figure 3, the authentication
17 software is not part of the secure part?

18 A. That's right, but you didn't ask me what was
19 stored in Figure 3. You asked me what can be in the
20 secure part of the BIOS, and I gave you an answer to
21 that question.

22 Q. Okay. So let me rephrase my question.

23 In Figure 3, what forms the secure part of the
24 BIOS?

25 A. In Figure 3, the secure part of the BIOS is

1 the encryption key stored in the BIOS, and also there
2 will be -- but this is more technical -- those functions
3 that give access at the start of the console and started
4 with secure parts.

5 Q. Is the secure part of the BIOS --

6 A. Yes.

7 Q. -- admitted to the encryption key?

8 A. Yes.

9 Q. I'm sorry, I didn't hear that. What was that?

10 A. Yes, that's the encryption key.

11 Q. So you -- you would agree that no other parts
12 of the BIOS, other than the encryption key, form the
13 secure part of the BIOS in Figure 3?

14 A. That's correct. Yes.

15 Q. And what do you think the patent means when it
16 says "secure area"?

17 A. I think it means the box and dotted lines in
18 Figure 3, "secure area." It's a part of memory which is
19 not accessible to the operating system where we have
20 authentication software, recovery application, secure
21 storage location, and then also block 58 which could,
22 for example, contain a log file of transactions.

23 Q. Is it correct that the authentication software
24 and other data that is shown in Figure 3 as being part
25 of the secure area that they're stored in inaccessible

THE SULLIVAN GROUP OF COURT REPORTERS

1 memory? Is that correct?

2 A. That's correct, because the BIOS will deny
3 access to the operating system of this area.

4 Q. And that inaccessible memory restricts access
5 to the operating system; is that correct?

6 A. That's correct.

7 Q. How is access to these memory locations
8 restricted?

9 A. This happens because the operating system
10 cannot just read a value as to the passing of the BIOS,
11 to ask access, and if the operating system requires
12 access to a secure area, the BIOS will deny this. So
13 it's the BIOS that regulates access to the secure area.

14 Q. So you had mentioned here that one of the
15 points of novelty in -- that the point of novelty --
16 sorry. Let me scratch that.

17 You had mentioned earlier that the point of
18 novelty of the '766 patent is that it provides this
19 separation that allows you to have a secure area that is
20 not accessible from -- by the operating system and that
21 that was something new in 2003.

22 Is that correct?

23 A. Well, that's only part of the story. The
24 newer thing is also that this is -- the secure part also
25 contains authentication software and can be used for

1 secure transactions.

2 Q. I'll have you turn to column 4, please,
3 lines 16 to 18. I'll read it. The sentence there says,
4 "A secure storage location and/or an encryption system
5 are not essential to the BIOS system with respect to the
6 present invention."

7 Is that correct?

8 A. That's correct.

9 Q. So how does the '766 system work without a
10 secure storage location?

11 A. Well, there is also the embodiment in Figure 5
12 where you actually modify the hardware and have secure
13 storage of keys and authentication software and hardware
14 in a separate hardware area.

15 Q. In that embodiment, the operating system can
16 access the authentication software; is that correct?

17 A. It cannot because access is mediated by the
18 BIOS, and, again, the BIOS will limit access to the
19 hardware. That's the role of the --

20 Q. Can a user -- sorry. Can a user access the
21 hardware?

22 A. No. Not directly. The user has to go to the
23 operating system. The operating system goes to the
24 BIOS, and then the BIOS goes to the hardware. And so
25 the BIOS mediates the access.

THE SULLIVAN GROUP OF COURT REPORTERS

1 Q. Which system is more secure, Figure 5A or
2 Figure 3?

3 A. I think it all depends on your threat level,
4 depending what the adversary --

5 (Court reporter requested clarification.)

6 THE WITNESS: Threat level, what the
7 assumptions are you make about the opponent. But, of
8 course, Figure 5 requires modifying the hardware, so it
9 will be more complex and expensive, but if it's done
10 well, it will give you a higher level of security
11 against certain attacks. For some other attacks, the
12 two systems are equivalent.

13 BY MR. KHAN:

14 Q. So you're saying that the embodiment in
15 Figure 5A, to be precise, is more secure than the one in
16 Figure 3?

17 A. I don't think that's what I said. I said for
18 certain attacks, this embodiment in Figure 5A will be
19 more resistant. Against other attacks, it will not make
20 a difference. It depends on your threat level whether
21 you care about the difference or not.

22 Q. So in looking at Figure 3 and Figure 5A of the
23 '766 patent, is it your understanding that the secure
24 area, Box 62 in Figure 3, is secure because it is
25 preventing access from the operating system?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Yes.

2 Q. And what would happen if a system in Figure 3,
3 for example, has multiple operating systems? Would
4 it -- would the secure area have to be protected from
5 all of the operating systems?

6 A. That is correct, yes.

7 Q. Can the console access the secure area?

8 A. It can access the data, but typically it will
9 only send instructions to the software running in secure
10 area and will make sure it actually runs as requested.
11 So actually it will recall API calls. It will give a
12 request to, for example, authenticate a piece of data
13 with a specific key and will get the answer. But there
14 is no need for the console to, for example, read the
15 keys. That's how you would implement the settings.

16 Q. So earlier you had mentioned that the console
17 is like an operating system.

18 A. It's a highly simplified operating system, so
19 it makes it easier to make it secure.

20 Q. Okay. So would it be fair to say that in some
21 cases you could have an operating system that speaks to
22 the secure area and other operating systems are not in
23 communication -- are prevented access to the secure
24 area?

25 A. I would consider it as a very bad design

THE SULLIVAN GROUP OF COURT REPORTERS

1 decision to replace a console by an operating system.

2 Q. And why is that?

3 A. Because operating systems typically are much
4 more complex, and more complex systems are more likely
5 to have bugs and flaws, and so you actually open
6 additional attack factors into your system. So
7 preferably the console should be as simple as possible.

8 Q. So a simple OS would do the job, not a complex
9 one; is that correct?

10 A. Well, I think simple OS is like an oxymoron.
11 OS has to do so many tasks. Typically OSs are not
12 simple.

13 Q. So I'm trying to understand, then. Is it then
14 your position that the console is not an operating
15 system?

16 A. It's a highly stripped-down operating system
17 with only very minimal functionality, and some experts
18 would no longer call it an operating system. That's why
19 they call it a console, because it doesn't have the
20 typical task that an operating system has.

21 Q. Okay. Thank you.

22 MR. KHAN: I think I'll pause there. Maybe we
23 can take our next ten-minute break. Does that sound
24 okay to everyone?

25 THE WITNESS: Fine for me.

THE SULLIVAN GROUP OF COURT REPORTERS

1 MR. HENRY: Fine.

2 (Recess: 10:17 a.m. to 10:32 a.m.)

3 BY MR. KHAN:

4 Q. Picking up where we were, turning to Figure 3,
5 Dr. Preneel, of the '766.

6 Do you have that in front of you?

7 A. Yes, I do.

8 Q. Great.

9 So Figure 3 shows a secure area 62 including
10 authentication software 54; is that correct?

11 A. That's correct.

12 Q. How does the authentication software get
13 stored in the secure area?

14 A. Can you clarify what you mean by "get stored"?
15 Get loaded in there or get stored in there, because --

16 Q. I mean, maybe you can clarify that. Is the
17 authentication software stored in the secure area, or is
18 it loaded in the secure area in the '766 patent?

19 A. Yes, this will be -- it depends on how the --
20 operator but will be in a separate part of memory that
21 is, as we discussed before, controlled by the BIOS and
22 not accessible to the operating system, and the
23 authentication software will be running in there. And
24 so I -- which is as a piece of RAM, so random access
25 memory which is separate, not accessible to the

1 operating system and where the software is run.

2 Q. So if I understood you correctly, you're
3 saying that the authentication software is stored in the
4 RAM where it's not accessible to the operating system;
5 is that correct?

6 A. Yes.

7 Q. And how does it get onto the RAM?

8 A. It will be loaded at boot time.

9 Q. At what time?

10 A. At boot time of the computer. At startup
11 time.

12 Q. I see.

13 So it's loaded there, and as a result, it's
14 stored onto the RAM and then --

15 A. Right.

16 Q. -- the BIOS protects it from the operating
17 system?

18 A. That's correct.

19 Q. Okay. Figure 5A, the authentication software
20 is in the hardware; is that correct?

21 A. That's correct.

22 Q. Which part of the hardware is it on?

23 A. Will be stored somewhere in -- I mean, there
24 can be many solutions. It doesn't -- I don't think it
25 necessary to specifically specify this in more detail,

1 but it can be nonvolatile memory somewhere.

2 (Court reporter requested clarification.)

3 THE WITNESS: Nonvolatile memory -- NVM,
4 nonvolatile memory, somewhere. But it can also be baked
5 into the hardware if your processor would be -- I mean,
6 processors have also -- can also have software run
7 inside the processor chip itself. It can be inside the
8 processor chip as well.

9 BY MR. KHAN:

10 Q. Sorry. It could be in a nonvolatile memory or
11 a ROM of the processor; is that correct?

12 A. That could be external or internal to the
13 processor.

14 Q. And if it's external to the processor, how is
15 it protected?

16 A. Well, in principle, the software only has to
17 be protected against modification, and then you would
18 use standard protection techniques. It's just the same
19 way as your boot software is protected through the
20 standard software authentication techniques with a
21 secure boot mechanism.

22 Q. So if a person of ordinary skill in the art
23 were to look at Figure 5A, I understand that the
24 authentication softwares and the hardware -- it's your
25 understanding that the possible implementations there

1 are one in which it could be part of the ROM in the
2 processor or one where it could be external to the
3 processor but with some standard well-known software
4 protection?

5 A. With boot protection -- with boot protection
6 mechanisms. But I think specifically if it would be
7 stored inside the processor, then no additional
8 protection would be needed because the processor area is
9 believed to be a secure area by itself.

10 Q. Okay. In -- in both in Figure 5A or Figure 3,
11 how is the authentication software stored and -- and so
12 I think in Figure 3 you said that it's a RAM, right? So
13 how is it stored? Where is it -- where does that code
14 come from that's creating this authentication software?
15 How does it create that memory space for the
16 authentication software?

17 A. I'm not sure I fully understand your question.
18 Memory space is allocated to this secure area, so you
19 don't have to create it. It's existing space in RAM.

20 Q. How is it allocated?

21 A. It's allocated because the BIOS decides which
22 space is for the regular operating system and user and
23 which part is for the secure part. So the allocation of
24 memory I understand is deciding which --

25 (Court reporter requested clarification.)

1 THE WITNESS: So the allocation is deciding
2 which part of the memory is for the applications and the
3 operating system on the one hand and which is for the
4 secure environment on the other hand, and this decision
5 is made by the BIOS.

6 BY MR. KHAN:

7 Q. And how does the BIOS determine which memory
8 spaces to allocate to a secure area and which ones to a
9 nonsecure area?

10 A. It depends on the size that's needed.
11 Typically, the secure area will be simpler because it
12 has less functions. It will get a smaller space than
13 the regular applications and operating system.

14 Q. Is it possible to change the configuration of
15 a system, for example, to store the authentication
16 software from in a secure area and then into the
17 hardware?

18 A. Figure 5A describes how authentication
19 software is stored into the hardware.

20 Q. Yes. My question was, is it possible, for
21 example, to change from Figure 3 to Figure 5A, or
22 Figure 5A to Figure 3, so you have the different places
23 where you might want to configure the authentication
24 software? Is that possible?

25 A. That's correct, but of course, for Figure 5,

1 you definitely have to change the hardware. So you
2 cannot just, for a given system, choose between one or
3 the other option. It's different design decisions.

4 Q. So is it correct to say that you could have a
5 system such as the one shown in Figure 3 and include the
6 authentication software in the secure area and
7 subsequently decide that you want to implement -- modify
8 that system so that you have the authentication software
9 in the hardware and therefore configure the hardware in
10 order to accommodate the authentication software? Is
11 that correct?

12 A. That would require a different design with
13 different hardware.

14 Q. And a different --

15 A. You have flexibility of where it was stored in
16 your design of authentication software; that's correct.
17 And if you store it -- you can store it in the option of
18 Figure 3 or you can store it in the hardware option of
19 Figure 5A. These are two embodiments of the invention.
20 Maybe it's important to point out that authentication
21 software itself need not be secret. You just have to
22 make sure that it's correct.

23 Q. Sorry. What need not be secret?

24 A. The authentication software itself.

25 Q. Authentication software itself. Okay.

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. Of course, the keys used in the software have
2 to be secret but not the software itself. It may be
3 secret, but it doesn't need to be secret.

4 Q. And in Figure 3, is the authentication
5 software secret or no?

6 A. Well, it it's in a protected environment, so
7 it could be secret.

8 Q. But is it or is it not?

9 A. It's an independent decision. The design does
10 not force you to make it public. You can make it public
11 and have this design, or you can keep it secret and have
12 this design.

13 Q. I see. So in Figure 3, the authentication
14 software, it may or may not be secret depending on the
15 design choice?

16 A. That's correct.

17 Q. And when you say "secret," are you using that
18 as another word for secure or, like, what are you --

19 A. Secret means it is available to the public for
20 inspection.

21 Q. And is it available to the operating system?

22 A. Well, you can hide it from the operating
23 system, or you can -- if it's available to the public,
24 obviously it's also accessible to the operating system.
25 I mean, it can run it itself --

THE SULLIVAN GROUP OF COURT REPORTERS

1 (Court reporter requested clarification.)

2 THE WITNESS: Yes. So I think it's a bit of a
3 rhetorical issue, so you can have the software secret or
4 not. It doesn't matter. It can be a public standard,
5 or it can be a proprietary secret standard. In both
6 cases, it's protected by secure area, but of course,
7 it's a public standard, everybody can know how it looks
8 like. That doesn't change the access of the operating
9 system. That's a different question.

10 BY MR. KHAN:

11 Q. I'm a little confused. If you could just
12 clarify the last two statements that were made. Reading
13 from the transcription, so I'll try to summarize, but
14 please feel free to correct me. I think you had
15 mentioned that if it's available to the public, it's
16 also accessible to the operating system; is that
17 correct?

18 A. This may be an unfortunate formulation.
19 Accessible, that's -- I mean, it's just available to
20 everybody, so also to the software, it doesn't mean the
21 operating system can run it, so I would say "accessible"
22 is not the correct term because "accessible" means the
23 operating system can run it.

24 Q. So the authentication software could be in the
25 secure area and be available to the public or may not be

THE SULLIVAN GROUP OF COURT REPORTERS

1 available to the public; is that correct?

2 A. That's correct.

3 Q. And when you say "available," what does that
4 mean?

5 A. The description is known. The code itself is
6 known.

7 Q. The code is known. I see.

8 A. Yeah.

9 Q. But your -- your position is that even though
10 the code may be known, the software itself cannot be
11 accessed by the operating system; is that correct?

12 A. That's correct. So the software, while being
13 run, cannot be inspected or accessed or stopped by the
14 operating system, and the operating system does not see
15 the particular values processed inside a secure area.

16 Q. So the authentication software that we are
17 referring to here, is that simply just allocated memory
18 spaces, or is there any data that is part of the
19 authentication software as well?

20 A. Authentication software is a computer program.
21 The computer program consists of instructions and data.

22 Q. So the authentication software is a program
23 that includes instructions and data; is that correct?

24 A. That's correct. Yes.

25 Q. So when you are loading the authentication

1 software to store it in the secure area, where is
2 that -- where is that data and instruction coming from?

3 A. That depends on the design. That could be in
4 the BIOS, or that could be also in an external memory.

5 Q. And after it's been stored in the
6 authentication -- sorry, in the allocated memory spaces,
7 is the authentication software generally removed from
8 the BIOS or the external memory?

9 A. No, it will remain there as well.

10 Q. Why?

11 A. Because that's -- the BIOS is a ROM memory.
12 It's memory you can only read and not write. So you can
13 load software from there, but after you load it, it will
14 still remain in there for next time you want to load it.

15 Q. If it's in the external memory, the external
16 memory gets deleted, does that affect the authentication
17 software in the secure area?

18 A. It would not affect it, but of course, if you
19 want to load it next time, it would no longer be
20 possible. So in practice, you would leave it there.

21 Q. So when your authentication software is coming
22 from an external memory, it is possible for that
23 external memory to get deleted and remove the
24 authentication software that was stored in that external
25 memory?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I don't think that makes sense from an
2 engineering point of view to do this.

3 Q. My question was, is it possible for the
4 external memory that stores the authentication software
5 to be deleted such that the authentication software is
6 no longer on the external memory?

7 A. That would happen, and then the next time you
8 boot the computer, it would no longer -- the process
9 would no longer work. It's similar as you would take a
10 smart card and destroy the smart card. Well, then you
11 can -- the next time, you cannot make -- you cannot use
12 it anymore.

13 Q. But the authentication software that's stored
14 in the secure area is still working even after the
15 external memory gets deleted, right?

16 A. Until -- yes, until the computer is booted
17 down.

18 Q. So whatever data is stored in the
19 authentication software remains there even though the
20 external memory might have been deleted; is that
21 correct?

22 A. That's correct, yes.

23 (Audio interruption.)

24 BY MR. KHAN:

25 Q. When the authentication software is stored in

THE SULLIVAN GROUP OF COURT REPORTERS

1 the allocated memory space, let's say it's coming from
2 external memory, how does that -- the -- does the -- is
3 the authentication software stored in a permanent memory
4 space necessarily?

5 A. I think we discussed this before. The
6 authentication software gets loaded from the nonvolatile
7 memory and gets then loaded into RAM --

8 (Court reporter requested clarification.)

9 THE WITNESS: From external memory, which is
10 nonvolatile memory, and gets stored into RAM, which is
11 obviously temporary memory.

12 BY MR. KHAN:

13 Q. And I think you had also said that in some
14 other implementations, it can be stored on the ROM --

15 A. That's correct, yes.

16 Q. -- in the processor; is that correct?

17 A. That's correct.

18 Q. And is the ROM temporary or permanent memory?

19 A. The ROM is permanent.

20 MR. KHAN: Just one second.

21 BY MR. KHAN:

22 Q. Could we turn to Claim -- so I'm hearing the
23 echo again.

24 Can we turn to Claim 1 of the '766.

25 Dr. Preneel, if could you let me know when you get

1 there.

2 A. That's fine. I have it in front of me.

3 Q. And in Claim 1, is it correct that the claim
4 recites, "The electronic device having an operating
5 system creating a run-time environment for user
6 applications and authentication software running in a
7 separate operating environment"? That's in column 18,
8 lines 13 to 16.

9 A. That's correct.

10 Q. Is that correct?

11 A. That's correct.

12 Q. Is it correct that Claim 1 does not recite a
13 BIOS?

14 A. That's correct.

15 (Audio disruption.)

16 BY MR. KHAN:

17 Q. Turning to paragraph 94 of your declaration,
18 Dr. Preneel, if you could let me know when you're there.

19 A. Yes.

20 Q. You have a statement in paragraph 94 saying,
21 about one, two, three -- seven -- six lines down,
22 "However, every such read/data retrieval involves some
23 sort of buffering: Most programming languages and
24 operating systems buffer at least part of the I/O
25 operations."

THE SULLIVAN GROUP OF COURT REPORTERS

1 Do you see that?

2 A. I see that, yes.

3 Q. What's your understanding of what "buffering"
4 means?

5 A. It means that there is no magic way to
6 immediately transfer a byte or a series of bytes from
7 the memory -- from one memory to the RAM of the
8 processor.

9 And memories are typically read off in larger
10 blocks and also the speeds of reading from the memory
11 and writing to the other location are not always the
12 same. So you have in between a buffer where information
13 that's transferred is stored in between information
14 being read from the source memory while -- before it's
15 being written to the destination memory.

16 Q. So is it correct that buffering -- when you're
17 reading and writing to a memory, where you're reading
18 data from one place and writing it to another place, due
19 to the relative differences of speed, read/write
20 operations, you would store the data on a buffer at
21 least temporarily until you could write it to the
22 destination allocated memory location; is that correct?

23 A. That's correct.

24 Q. And how long does the buffering normally take?

25 A. That depends on the relative speeds and on the

THE SULLIVAN GROUP OF COURT REPORTERS

1 data sizes, of course.

2 Q. Could you give me an example?

3 A. Of course. I think main memory read speeds
4 are on the order of -- data does not come from cache
5 memory. It's hundreds of nanoseconds or delays before
6 data can be read, and data comes also in quite large
7 blocks. For example, if you --

8 (Court reporter requested clarification.)

9 THE WITNESS: -- if you read from hard disks,
10 then it comes in blocks of 512 bytes, and this is
11 typical order. It might be due to buffer, it needs to
12 have several of those blocks, and so this is order of
13 magnitude of those things. So you may have to store
14 data for milliseconds and you may have to buffer
15 kilobytes of data.

16 BY MR. KHAN:

17 Q. So while maybe -- so because you read --
18 correct me if I'm wrong. As you're reading certain
19 chunks of memory and you'd store those chunks until you
20 were able to write those chunks of memory and perhaps
21 the duration of storage in the buffer may depend on the
22 speed of your processor and the --

23 A. The latency and the speeds of the memory
24 reads.

25 (Court reporter requested clarification.)

THE SULLIVAN GROUP OF COURT REPORTERS

1 BY MR. KHAN:

2 Q. Okay. Can I ask you to open up the Ellison
3 reference? That's Exhibit 1006, please.

4 A. Yes, I have it in front of me.

5 Q. Okay. And then may I ask you to turn to
6 Figure 1C, please.

7 A. Can you repeat that? 1C?

8 Q. 1C, yes.

9 A. Okay. At this time I have that, yes.

10 Q. Okay. Thank you.

11 In Figure 1C, is it correct that there is a
12 mass storage device 170?

13 A. Yes, that's correct.

14 Q. Is it correct that the system that's shown in
15 Figure 1C also includes a CD-ROM 172, floppy drive 174,
16 hard drive 176?

17 A. That is correct.

18 Q. Is it also true that this system includes I/O
19 devices 175?

20 A. Yes, it does.

21 Q. Is it also correct that it includes a
22 nonvolatile memory 160 that includes a processor nub 18?

23 A. Yes, it does.

24 Q. And typically what types of devices may be the
25 I/O devices 175?

1 A. Of course, you have to go back a while. I
2 guess it could have been screens or printers. At that
3 time, we also -- I think we started seeing USB ports.

4 Q. And how about nonvolatile memory? What -- do
5 you know what -- typically what would a nonvolatile
6 memory be like, or what are different implementations of
7 a nonvolatile memory?

8 A. A nonvolatile memory is typically an E2PROM I
9 see with -- that can store information. It can also be
10 rewritten. But even if the device overall loses power,
11 the information stays in the memory.

12 Q. Is it correct that the nonvolatile memory can
13 be a flash memory?

14 A. Yes, E2PROM is the same as flash, for your
15 clarification. That's the informal name for E2PROM
16 memory.

17 Q. Is the system in Ellison, through the I/O
18 devices, capable of communicating with another device?

19 A. Yes, it can.

20 Q. In Figure 1C, do you see the ICH unit,
21 input/output controller hub, 150?

22 A. Yes, I see this.

23 Q. What's the operation of the ICH 150?

24 A. Can you clarify the question? You mean the
25 function? You mean how it works? What the goals are?

THE SULLIVAN GROUP OF COURT REPORTERS

1 Or what specifically do you want to know?

2 Q. Yeah, so maybe I can -- I can be a little more
3 precise here. Excuse that.

4 The ICH 150 includes a processor nub/executive
5 loader; is that correct?

6 A. That's correct.

7 Q. Do you know what that loader -- how does that
8 loader work -- loader at 52 work?

9 A. Well, I think that refers there to look at
10 Figure 1A where it shows where this processor
11 nub/executive loader is located in the isolated
12 execution environment of Ellison and more specifically
13 in the Ring-0.

14 (Court reporter requested clarification.)

15 BY MR. KHAN:

16 Q. Okay. And you mentioned the isolated
17 environment.

18 What's -- scratch that. Sorry. The -- so
19 system Figure 1 -- sorry.

20 Figure 1C also shows an MCH, the memory
21 controller hub 130; is that correct?

22 A. That's correct.

23 Q. Is it possible to have multiple MCHs and
24 multiple ICHs in Ellison's system?

25 A. As an engineer, I would say, yes, it's

THE SULLIVAN GROUP OF COURT REPORTERS

1 possible. My general opinion is that the Ellison design
2 is incredibly complex, and to have the value of making
3 it even more complex is hard to see. But technically it
4 would be feasible.

5 Q. And can the MCH be integrated with the ICH?

6 A. You can do that, but then you have a different
7 design, but again different considerations, different
8 security requirements. You can take all these blocks
9 here and combine them in different ways, and you every
10 time have different designs with different properties.

11 Q. Okay. Can I turn your attention to column 4
12 of Ellison at lines 46 to 51.

13 A. Okay. Shall I read it?

14 Q. Yes, please.

15 A. "The MCH may be integrated into a chipset that
16 integrates multiple functionalities such as the isolated
17 execution mode, host-to-peripheral bus interface" --

18 (Court reporter requested clarification.)

19 THE WITNESS: -- "host-to-peripheral bus
20 interface, and memory control."

21 I think that's --

22 BY MR. KHAN:

23 Q. Could you read the next line too, please.

24 A. "Similarly, the ICH may also be integrated
25 into a chipset together or separate from the MCH to

1 perform I/O functions."

2 I think that's consistent with my statement
3 that you can combine these things. There is still
4 different engineering approaches whether you combine
5 those as separate building blocks on the same chip or
6 multiple chips in a larger encapsulation or whether you
7 really integrate this into a single device. And, yes,
8 all these options are possible, and you actually get
9 designs, I would argue, with different security and
10 performance properties.

11 Q. I see.

12 So when the memory controller, MCH, is
13 designed separately from the ICH and then compare that
14 to the scenario where they're integrated together, is
15 it -- is it accurate to say that the combined unit of
16 the MCH and the ICH would be performing functions that
17 are greater than just memory control? Right? That they
18 would incorporate some of the functionalities of the ICH
19 as noted in the blocks in Figure 1C such as the isolated
20 execution logical processing manager and the other units
21 there, the token bus interface.

22 Is that a fair statement to say that when you
23 combine these two units, essentially perform the
24 combination of the two, would it be limited to any one
25 particular operation?

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I think it would indeed be possible to combine
2 these two in one operation, although I think in
3 practice, you would still have two separate -- it would
4 still be implemented in practice as two separate units
5 inside the same housing or inside the same -- because
6 their functions are very different.

7 Q. Okay.

8 MR. KHAN: I think we've come up to the
9 one-hour mark. So I like using this as a good place to
10 take a short break and come back in ten minutes, if that
11 works for everyone.

12 THE WITNESS: That's fine.

13 MR. HENRY: Fine with me.

14 (Recess: 11:19 a.m. to 11:27 a.m.)

15 MR. KHAN: We have no further questions. So
16 if Mr. Henry would like to redirect, or its his now.

17 MR. HENRY: Excellent. I do have a few
18 questions.

19 EXAMINATION BY MR. HENRY:

20 Q. Dr. Preneel, can you please clarify what is
21 the console in the '766 patent?

22 A. So the console is a simple piece of software
23 that is being called by the BIOS and that manages access
24 to the secure area. And so this console provides
25 application programming interface, so an interface to

1 which calls can be made to authenticate specific
2 transactions. It would even be possible in this case to
3 actually go directly from user application to this --

4 (Court reporter requested clarification.)

5 THE WITNESS: I will repeat slowly.

6 It would be possible to also go directly from
7 user application to the console API and bypassing the
8 BIOS because the console can also manage access to the
9 secure area.

10 BY MR. HENRY:

11 Q. All right. Then what distinguishes the
12 console as depicted in Figure 3 from that depicted in
13 Figure 5A?

14 A. Obviously in Figure 3, the console gets access
15 to the secure area which is sitting in software above,
16 and the console provides application interface to calls,
17 for example, authentication software to authenticate
18 transactions. In Figure 5, this authentication software
19 is implemented in the hardware environment, and so if
20 you would make from the user application a call to
21 console, it would then call BIOS and hardware to get
22 authentication software run.

23 So it remains the central place to invoke the
24 authentication software. In Figure 3 is application --
25 authentication software runs in secure area in RAM. In

1 Figure 5A, it runs in the hardware environments.

2 Q. I'd like you to turn your attention to the
3 subject of the keys, specifically the encryption key.

4 How does the use of the encryption key as set
5 forth in the '766 patent -- what's -- let me be more
6 specific.

7 In the embodiment that's more or less depicted
8 in Figure 3 of the '766 patent, we have an encryption
9 key, but you did agree that, you know, keys preexisted
10 this patent application. So how does the use of the
11 encryption key in the '766 patent, at least as depicted
12 in Figure 3, how does it make -- count as a step forward
13 distinguishing it from the prior art?

14 A. Because first, this encryption key makes this
15 BIOS unique and specific for a particular user device or
16 a particular user. And second, this BIOS encryption key
17 can be used in the secure area to access other keys or
18 it could also be used in principle in authentication
19 software because a cryptographic key is a bit string
20 that can also be used with authentication software. But
21 typically, I would say it would be used to control
22 access to other keys, and so it helps to protect the
23 secure area and the key material in the secure area.

24 Q. All right. So how does that -- what you just
25 described, how does that differentiate the claims of the

1 '766 patent, or specifically, say Claim 1, from the
2 disclosure of Ellison?

3 MR. KHAN: Objection -- sorry. Objection.
4 Form. And these -- the scope of the redirect should be
5 based on the questions that I asked.

6 MR. HENRY: Well, you asked about Ellison.

7 MR. KHAN: I did not ask how they
8 differentiated from Claim 1, which is your question.

9 MR. HENRY: All right. Are you going to let
10 him answer the question?

11 THE WITNESS: So in Claim 1, in '766, a
12 private key is provided in the secure area of the
13 electronic device where it's inaccessible to the user
14 and it's inaccessible to the operating system and it's
15 also inaccessible to the users, and it can be directly
16 used in an electronic transaction to protect the
17 transaction of the user.

18 The Ellison patent also uses obviously
19 cryptographic keys, but those keys are used to
20 protect -- to separate and protect the secure
21 environment from the regular environment. That's the
22 fundamental difference.

23 BY MR. HENRY:

24 Q. Okay. You were asked previously, I think,
25 about -- I'm paraphrasing, of course, but -- your

1 comment about -- in your declaration, you made a comment
2 about the '766 patent being -- serve as a major step
3 forward or having major steps forward over the prior
4 art, right?

5 A. That's correct, yes.

6 Q. Can you please clarify again what are the
7 major steps over the prior art?

8 A. I think the prior art was that, as I
9 mentioned, people were doing transactions online
10 already, and they're doing transactions in the physical
11 world using bank cards, and online transactions were
12 performed using browsers, and without providing a secure
13 environment, which meant that if your device was
14 compromised by malware, that would affect the user
15 application or the operating system. That could also
16 compromise transactions and lead to fraudulent
17 transactions.

18 And so by providing in a simple and elegant
19 way a secure environment, '766 makes it possible -- I
20 think it's particular on an existing device without
21 adding complex and expensive hardware and changing all
22 of the software, but just software changes allowed
23 secure transactions on an ordinary machine. It also
24 provided options with much simpler hardware changes to
25 provide secure transactions on an ordinary machine.

1 So I think many people had ideas on how to
2 build very complex architectures for much more secure
3 computers with secure and less secure environments, but
4 '766 shows it's possible that if one focuses on
5 transactions, and not on complete computer
6 architectures, to actually have a simple and elegant
7 solution that provides the necessary isolation and
8 protection.

9 Q. During your earlier testimony, you discussed
10 the topic of the authentication software possibly
11 being -- for example, that's Number 54, authentication
12 software -- being -- you used the term "public but
13 nevertheless secure."

14 A. Yes.

15 Q. Can you please explain, at least for my
16 edification, how it can be both public and secure?

17 A. It's important to understand that in
18 cryptography there is an important principle called
19 Kerckhoffs' principle -- K-E-R-C-K-H-O-F-F-S,
20 apostrophe, the name is Kerckhoffs -- which states that
21 the cryptographic method should remain secure, even if
22 the algorithm itself is publicly known. The security of
23 the algorithm should only rely on the secrecy of the
24 key. And so authentication algorithm can be public,
25 also the software or hardware implementing

1 authentication algorithm can be public. One only needs
2 a secret key in the software to get protection of the
3 transaction.

4 And in that sense, it does not matter whether
5 the authentication software in the form of software --
6 software is actually public or not. Even if it's made
7 publicly available for inspection, even if it follows a
8 common standard, still the provided solution can be
9 secure under the condition that there is a secret key in
10 the secure area that can be input to the authentication
11 software.

12 MR. HENRY: I don't have any more redirect
13 questions. I pass the witness.

14 MR. KHAN: Thank you. I have one or two quick
15 follow-up questions.

16 FURTHER EXAMINATION BY MR. KHAN:

17 Q. Dr. Preneel, you mentioned early in the
18 redirect that the -- the BIOS could be bypassed because
19 the console has the capabilities by itself to restrict
20 access; is that correct?

21 A. That is correct, yes.

22 Q. Can you point to me where in the '766 patent
23 it says the BIOS can be bypassed?

24 A. I'm afraid I would need more time to look this
25 up.

1 Q. You can take your time.

2 A. I'm afraid that I can't point to a specific
3 passage, but I also don't find the place where this
4 would be made impossible.

5 Q. So what I understand you are saying is that
6 your characterization of the BIOS was not something you
7 found disclosed in the patent but something that you
8 think is within the realm of possibility; is that
9 correct?

10 A. This was a specific comment where we pointed
11 out that one could implement the whole system also in
12 bypassing the BIOS. I think what I said previously
13 about the BIOS is still correct. That's essentially the
14 BIOS -- and this is also what follows on Figure 3, that
15 normally the user application goes to the OS and the
16 BIOS, and the BIOS plays the role of separator or
17 decider who gets access to the secure part of the
18 memory.

19 Q. I can appreciate that. I think my comment was
20 more directed towards, you know, the bypassing of the
21 BIOS, right, and the console being able to fill in for
22 the BIOS. And I think you were unable to find support
23 when asked, and that's why I was clarifying your
24 position in that you think it's possible, but it's not
25 disclosed.

THE SULLIVAN GROUP OF COURT REPORTERS

1 A. I could not point, indeed, to a location where
2 it is disclosed.

3 Q. Thank you.

4 Also, was there anything in the redirect
5 that -- Mr. Henry just asked you the questions. Was
6 there anything in the redirect that contradicted what
7 you said earlier, or do you think it was consistent with
8 your --

9 A. I think it was consistent. I've tried my very
10 best to be consistent. To the best of my recollection,
11 I have been consistent.

12 MR. KHAN: Thank you very much. I have no
13 further questions.

14 THE WITNESS: Thank you.

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

17 MR. KHAN: Yes, if we could get a rough draft,
18 like, soon -- like, as soon as possible, and then when
19 do you think we can get the official transcript by?

20 COURT REPORTER: When would you like it?

21 MR. KHAN: What are the options?

22 COURT REPORTER: May we go off the record?

23 (Discussion off the record.)

24 THE REPORTER: And, Mr. Henry, did you want a
25 copy, sir?

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

MR. HENRY: Yes, please.

(Whereupon the proceedings concluded at 11:48
a.m.)

THE SULLIVAN GROUP OF COURT REPORTERS

1	ERRATA SHEET		
2	NAME OF CASE: SAMSUNG ELECTRONICS CO., LTD. V. WARD		
3	PARTICIPATIONS B.V.		
4	DATE OF DEPOSITION: NOVEMBER 1, 2022		
5	NAME OF WITNESS: DR. BART PRENEEL		
6	Reason Codes:		
7	1:	To clarify the record.	
8	2:	To conform to the facts.	
9	3:	To correct transcription error.	
10	Page	Line	Reason
11	From	to	
12	Page	Line	Reason
13	From	to	
14	Page	Line	Reason
15	From	to	
16	Page	Line	Reason
17	From	to	
18	Page	Line	Reason
19	From	to	
20	Page	Line	Reason
21	From	to	
22	Page	Line	Reason
23	From	to	
24	DR. BART PRENEEL		
25	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 1, 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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 20
- 21
- 22
- 23
- 24
- 25

THE SULLIVAN GROUP OF COURT REPORTERS

Index: 'BRI'..8

<p>'</p> <p>'BRI' 32:5 35:12</p> <hr/> <p>-</p> <p>--o0o-- 6:2</p> <hr/> <p>1</p> <p>1 6:1 28:7 29:13 82:24 83:3,12 88:19 94:1,8,11</p> <p>10 13:18,22 19:23 20:6,15 27:7,9,16 37:13,25</p> <p>1001 10:10</p> <p>1006 48:22 86:3</p> <p>10:17 71:2</p> <p>10:32 71:2</p> <p>11,063,766 10:9</p> <p>11,603,766 10:4</p> <p>11:19 91:14</p> <p>11:27 91:14</p> <p>13 83:8</p> <p>130 88:21</p> <p>14 44:16</p> <p>150 87:21,23 88:4</p> <p>16 67:3 83:8</p> <p>160 86:22</p>	<p>170 48:20 86:12</p> <p>172 48:20 86:15</p> <p>174 48:21 86:15</p> <p>175 86:19,25</p> <p>176 48:21 86:16</p> <p>18 12:24,25 13:2 67:3 83:7 86:22</p> <p>1993 40:9 53:5</p> <p>1A 88:10</p> <p>1C 86:6,7,8,11,15 87:20 88:20 90:19</p> <hr/> <p>2</p> <p>2.0 24:13</p> <p>20 31:11,14,22 32:10,14, 16 35:4 51:20,25</p> <p>2000 24:2</p> <p>2003 54:12,20,22 55:20,21 56:6 66:21</p> <p>2004 44:7,17</p> <p>2008 44:7</p> <p>2009 9:24 34:24 35:3 44:8 48:23,25 49:4</p> <p>2022 6:1</p> <p>21 32:14</p> <p>22 32:2,11,17 35:10 36:19</p>	<p>37:22</p> <p>24 48:14</p> <p>250 48:15 49:10,12</p> <p>29 40:11</p> <hr/> <p>3</p> <p>3 58:15 59:22 60:12,20 64:13,16,19,23,25 65:13,18,24 68:2,16,22, 24 69:2 71:4,9 74:10,12 75:21,22 76:5,18 77:4, 13 92:12,14,24 93:8,12 98:14</p> <p>30 12:5</p> <p>31 58:9</p> <p>321 31:17</p> <hr/> <p>4</p> <p>4 67:2 89:11</p> <p>41 50:11</p> <p>46 60:23 89:12</p> <p>48 61:19</p> <p>480 22:23 36:12 44:19,21</p> <hr/> <p>5</p> <p>5 27:7 67:11 68:8 75:25 92:18</p> <p>50 50:3</p> <p>51 89:12</p>	<p>512 85:10</p> <p>52 48:17 88:8</p> <p>54 48:23 49:1,6,9,16 71:10 96:11</p> <p>58 65:21</p> <p>5A 68:1,15,18,22 72:19 73:23 74:10 75:18,21, 22 76:19 92:13 93:1</p> <hr/> <p>6</p> <p>6 60:25</p> <p>61 61:2,3</p> <p>62 60:25 61:2,3 64:14 68:24 71:9</p> <hr/> <p>7</p> <p>7 45:14,17</p> <p>72 50:3</p> <p>766 9:1 14:7,14 15:5 16:23 17:22,24 18:25 19:9 22:23 27:19,20 28:6 29:6 32:8 36:12,16 42:24 43:7 44:16 50:8, 12,19,25 52:15 58:10 60:12,20 63:12 66:18 67:9 68:23 71:5,18 82:24 91:21 93:5,8,11 94:1,11 95:2,19 96:4 97:22</p> <p>776 44:15</p> <hr/> <p>8</p> <p>8 22:17,22 23:7 27:9</p>
---	---	--	--

80 27:6 80s 24:21 53:19 8:06 6:1 <hr/> <p style="text-align: center;">9</p> <hr/> 90s 26:16 53:23,24 55:10 93 55:9 94 53:5 55:9 83:17,20 95 55:9 9:12 45:9 9:24 45:9 <hr/> <p style="text-align: center;">A</p> <hr/> a.m. 6:1 45:9 71:2 91:14 ability 30:1 abroad 13:5 academia 17:14 academic 16:24 17:10,18 access 28:14 29:23 50:21 57:25 58:23 59:7,17,21, 23,25 61:23,25 62:2,4, 5,8,9,13,14,15 63:18, 19,22 65:3 66:3,4,7,11, 12,13 67:16,17,18,20, 25 68:25 69:7,8,23 71:24 78:8 91:23 92:8, 14 93:17,22 97:20 98:17 accessed 79:11,13	accessible 29:1 65:19 66:20 71:22, 25 72:4 77:24 78:16,19, 21,22 accessing 59:2 accommodate 76:10 accurate 61:16 90:15 achieve 16:11 acquired 40:1 act 31:7 actions 61:15 active 24:20 59:12 add 26:7 51:16 added 24:8 51:13,15 adding 95:21 addition 58:19 additional 50:15 51:2,4,11,18 52:4,18 70:6 74:7 admitted 65:7 advanced 38:6 41:2 adversary 68:4 advising 12:15 advisor 24:6 affect 80:16,18 95:14 afraid 97:24 98:2	age 41:15 agree 8:7,11 18:6 46:4,6,14, 16 49:1 65:11 93:9 ahead 7:21 Al-salqan 45:17 algorithm 16:6 23:4 55:17 96:22, 23,24 97:1 algorithms 13:25 14:10,15 15:8,17 16:4,13,15,25 17:15,20 22:10 37:14 38:1 53:17 55:1 Alliance 24:4 allocate 75:8 allocated 74:18,20,21 79:17 80:6 82:1 84:22 allocation 74:23 75:1 allowed 8:3 95:22 analysis 15:23 and/or 67:4 anymore 81:12 API 59:5 69:11 92:7 apologies 12:22 apology 12:23 apostrophe 96:20 applicability 12:16 application	43:1 53:1 58:21 65:20 91:25 92:3,7,16,20,24 93:10 95:15 98:15 applications 28:10,13,23 30:20,23 54:13,14 56:16,19,21 57:6 75:2,13 83:6 applied 26:17,24 27:5 39:6 applies 18:12 apply 12:17 18:19 31:25 32:7 37:8 43:5 approaches 51:3 90:4 arbitration 11:1,4,5,11 13:10,15 architecture 38:12,24 55:21 architectures 96:2,6 area 17:10 18:23 23:21 26:13 27:22,24 29:2 40:16 58:2,17 59:2,25 60:2 64:14 65:16,18,25 66:3,12,13,19 67:14 68:24 69:4,7,10,22,24 71:9,13,17,18 74:8,9,18 75:8,9,11,16 76:6 78:6, 25 79:15 80:1,17 81:14 91:24 92:9,15,25 93:17, 23 94:12 97:10 areas 13:24 15:3 20:16,24 21:5,16 37:13,24 60:5 argue 90:9 arguments 47:4 art 36:22,25 37:11,22 38:17 39:16,22 40:3,14, 19,20 42:11 44:11 73:22 93:13 95:4,7,8 articles 43:15
--	--	---	--

asks 62:23 aspects 21:19 assume 39:5 assumptions 68:7 asymmetric 55:15 attack 70:6 attacks 52:24 68:11,18,19 attempt 47:3 attention 89:11 93:2 attorney 7:6 audio 81:23 83:15 authenticate 29:5 69:12 92:1,17 authentication 27:23 28:22 55:2,14 58:18,23 61:4 64:7,8, 11,14,16 65:20,23 66:25 67:13,16 71:10, 12,17,23 72:3,19 73:20, 24 74:11,14,16 75:15, 18,23 76:6,8,10,16,20, 24,25 77:4,13 78:24 79:16,19,20,22,25 80:6, 7,16,21,24 81:4,5,13, 19,25 82:3,6 83:6 92:17,18,22,24,25 93:18,20 96:10,11,24 97:1,5,10 authorize 56:17 avoid 12:18 aware 40:24 55:25	<hr/> B bachelor 37:5 38:5 39:14,18,24 40:24,25 42:1,8,10,17 bachelor's 37:12,23 38:17 41:22 back 22:17 51:20 52:13 58:8 87:1 91:10 bad 69:25 baked 73:4 bank 51:22 52:2 56:11 95:11 banking 53:19 55:4 56:3,14,15, 16 banks 55:24 56:2 BART 6:7 based 42:6 43:11 54:25 55:15, 16 94:5 basic 14:17 37:3 38:11 59:11 basis 40:22 41:8 Belgium 13:5,11 54:3,5,6 believed 74:9 big 27:4 BIOS 51:8 59:3,4,7,10,11,14, 15,17,21,24 60:5,6,8, 13,15,16,19,21 61:5,7, 12,17,21,24 62:11,12, 18,19,20,24 63:2,5,8, 10,13,18,21 64:2,15,16, 20,24,25 65:1,5,12,13 66:2,10,12,13 67:5,18, 24,25 71:21 72:16 74:21 75:5,7 80:4,8,11	83:13 91:23 92:8,21 93:15,16 97:18,23 98:6, 12,13,14,16,21,22 bit 16:7,8 29:9 36:10 61:20 78:2 93:19 Black 9:12 block 65:21 blocks 17:4 84:10 85:7,10,12 89:8 90:5,19 board 31:15 35:5 boot 61:14 72:8,10 73:19,21 74:5 81:8 booted 81:16 boots 59:12 box 47:24 65:17 68:24 break 7:16,18 15:17 45:1,11 70:23 91:10 breaks 7:14,16 8:2 BRI 32:7 35:15 36:20 briefs 8:22 bring 26:6 broadest 32:4 35:11 broken 16:21 browser 52:21,25 53:5,7 56:23 58:21 browsers 52:18 95:12 buffer	83:24 84:12,20 85:11, 14,21 buffering 83:23 84:3,16,24 bugs 70:5 build 15:25 17:5 96:2 building 17:4 90:5 bus 89:17,19 90:21 business-to-business 56:20 bypassed 97:18,23 bypassing 92:7 98:12,20 byte 84:6 bytes 84:6 85:10
			<hr/> C cache 85:4 call 53:17 55:1 58:5 59:5 62:24 63:5 70:18,19 92:20,21 called 6:8 24:3 31:8,9 59:6 91:23 96:18 calls 69:11 92:1,16 capabilities 97:19 capable 87:18 card 51:21,23 52:2,3,4,23 53:21 55:6,8 56:11,13, 14,17 57:20 58:25 81:10

THE SULLIVAN GROUP OF COURT REPORTERS

Index: cards..confusion

cards 23:22,23 54:7 55:4,5,6 95:11 care 68:21 carefully 17:6 carried 52:18 case 12:18 13:9 25:6 28:8 37:7 43:1 47:9 55:2 64:13 92:2 cases 13:5,8,11,15 38:6 59:23 69:21 78:6 CD-ROM 48:20 86:15 central 92:23 challenged 31:20 35:25 change 9:20 75:14,21 76:1 78:8 changing 95:21 channel 53:7,9,12 characterization 98:6 chat 33:8 47:24 chip 73:7,8 90:5 chips 90:6 chipset 89:15,25 choice 77:15 choose 76:2 chunks 85:19,20	circuits 51:17 citation 26:3,8 48:25 49:1 50:4 citations 26:8 48:18 49:19 cite 25:5,11,23 48:22 cited 9:4 claim 21:24,25 28:1,7 29:13 36:20 82:22,24 83:3,12 94:1,8,11 claimed 50:19 claims 19:1,9 21:9,12 22:9 27:20 31:20 32:3,18 33:1 35:11,25 50:12 93:25 clarification 12:1,19 14:22 15:12 19:18 22:5 24:15 25:13 28:20 37:15 47:15 49:11 51:24 54:4 64:10 68:5 73:2 74:25 78:1 82:8 85:8,25 87:15 88:14 89:18 92:4 clarify 12:10 13:6 17:12 22:14 25:24 71:14,16 78:12 87:24 91:20 95:6 clarifying 98:23 clarity 21:10 classes 26:14,17,22 27:1,4,11 clauses 12:6 clear 9:16 19:25 20:12,19 27:25 36:8 57:6,18 code 30:10 62:14,15,18 74:13 79:5,7,10	codes 55:2 coin 15:24 16:6,17 18:5 colleague 6:21 colleagues 43:8 column 60:25 67:2 83:7 89:11 combination 45:19 90:24 combine 89:9 90:3,4,23 91:1 combined 55:14 90:15 comment 95:1 98:10,19 comments 47:4 common 97:8 communicate 45:12 communicates 8:8 61:18 communicating 87:18 communication 69:23 companies 11:20 12:4,15 compare 90:13 complete 51:6 96:5 completion 42:8 complex 56:18 60:6,7 61:20 68:9 70:4,8 89:2,3 95:21 96:2 complexity 43:3	components 18:4 19:6 43:19 63:20, 23 64:2 compromise 95:16 compromised 28:15 29:21,22 58:22 95:14 computation 28:21 computations 51:20 compute 29:4 54:7 computer 28:6 31:5 38:9,12,14, 22,24 39:1 52:21 58:25 59:13,15,19 72:10 79:20,21 81:8,16 96:5 computers 39:4 96:3 computing 24:4 29:3 concern 33:11,13 concerns 43:6 concluded 8:5 condensed 27:6 condition 97:9 configuration 75:14 configure 75:23 76:9 confirm 10:12 34:19 42:7 48:11 49:4 confirmed 49:5 confused 78:11 confusion
---	---	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: connect..decryption

12:22 20:20,21 33:18	copy 9:3,4 33:7 34:15,21,24 47:17 48:3 50:7 99:25	courses 27:13 38:14,23,24 39:1	CS 38:23
connect 56:13	copyright 13:12	court 6:5 12:1 13:5,8,9,11,15 14:22 15:12 19:18 22:5 24:15 25:13 28:20 34:16 37:15 45:8 47:15 49:11 51:24 54:4 64:10 68:5 73:2 74:25 78:1 82:8 85:8,25 88:14 89:18 92:4 99:15,20,22	curriculum 27:10
connection 62:10	core 62:7	cover 10:3,14	cybersecurity 38:14 39:6
considerations 89:7	correct 6:20 7:8,9 9:10 10:5,6, 7,11,16,17 11:10,13,14 13:14,16,17 14:5,6 22:25 23:1,5,6,10,11 26:2 30:24 31:22,23 32:5,6 33:1,4 35:4,8,9, 13,14,16,17 36:23,24 38:20 39:19 40:10,12 41:19,23,24 43:12,13 44:17,18 45:21,22 47:10,12,13 48:13,23, 24 49:17,18,20,21,23, 24 50:1,2,4,5,16,17,23, 24 52:10 54:14 57:11, 12 59:24 60:1,3,4,22 61:2,3 65:14,23 66:1,2, 5,6,22 67:7,8,16 69:6 70:9 71:10,11 72:5,18, 20,21 73:11 75:25 76:4, 11,16,22 77:16 78:14, 17,22 79:1,2,11,12,23, 24 81:21,22 82:15,16, 17 83:3,9,10,11,12,14 84:16,22,23 85:18 86:11,13,14,17,21 87:12 88:5,6,21,22 95:5 97:20,21 98:9,13	covered 27:11	<hr/>
consists 15:23 61:21 79:21	correction 46:15	create 28:24 29:25 74:15,19	D
console 30:8,12,15,18,22 31:7,9 58:16 65:3 69:7,14,16 70:1,7,14,19 91:21,22, 24 92:7,8,12,14,16,21 97:19 98:21	correctly 6:18 52:9 60:20 72:2	created 53:6 55:9	daily 40:22
consult 41:8	counsel 6:3 10:21,23 33:20,22 45:12 47:1 99:15	creating 58:13,25 74:14 83:5	data 50:22 52:20 55:14 62:21,22,25 64:7 65:24 69:8,12 79:18,21,23 80:2 81:18 84:18,20 85:1,4,6,14,15
consultations 47:6	Counselor 63:15	credit 52:23 53:21 55:6,8	date 44:5,16,20 52:14
consulted 11:19	count 93:12	cross-examination 8:4,9	deal 41:9
consumer 56:21	countries 54:3	cryptanalysis 14:1,10 15:4,7 16:4,14 22:11 37:14 38:2 39:9, 10	debit 55:5,6
content 18:20	country 54:5	cryptanalyze 15:16	decide 18:17 76:7
contents 34:12 46:4,7 47:1		crypto 57:17	decider 98:17
context 21:8 22:14 27:16 53:14		cryptographers 53:17 55:1	decides 63:21 74:21
continue 37:19		cryptographic 13:25 14:2,9,11,15,20 15:8,13,14,17 16:3,6,9, 12,13 17:19 22:8,10 23:4,15 37:14 38:1,3 43:18 44:1 51:19 53:2, 4,9 64:6 93:19 94:19 96:21	deciding 74:24 75:1
contradicted 99:6		cryptography 15:21,23,25 26:17,24, 25 27:5 38:15 39:6 53:10 54:25 96:18	decision 70:1 75:4 77:9
control 16:9 89:20 90:17 93:21			decisions 76:3
controlled 71:21			declaration 8:25 9:4,11,12,20,23 10:3,4,18 12:24 13:18, 19 20:2,19,22 22:17 25:5,12,22 26:4,15 31:11 36:16 40:17 45:15 46:2,3,8,18,19,25 47:1 49:2,4,7 50:3,11 83:17 95:1
controller 87:21 88:21 90:12			decrypted 58:19
conversations 43:11			decryption

THE SULLIVAN GROUP OF COURT REPORTERS

Index: dedicated..easier

57:21 58:4	deposition 8:17,20 10:19 25:12 36:9 46:16	47:11 68:20,21 94:22	disruption 83:15
dedicated 27:13	describes 75:18	differences 84:19	distinguishes 92:11
deemed 56:18	description 21:20 49:25 79:5	differentiate 93:25	distinguishing 93:13
deficiencies 45:18	design 13:25 15:23 16:19 18:6 37:25 59:22 60:11 69:25 76:3,12,16 77:9, 11,12,15 80:3 89:1,7	differentiated 94:8	divided 60:21
define 20:24 21:1	designed 24:18 90:13	difficulties 43:6	division 30:2
defined 19:13 61:11	designs 60:7 89:10 90:9	digital 9:6,9 50:22 53:13,15,20 54:1,6,8,12,19,22 55:10,15,16 56:3	doctor's 40:7
definition 22:2 37:2 53:16	destination 84:15,22	directed 98:20	doctorate 40:2
degree 37:5,6,12,24 38:5,18 39:2,14,20,24,25 40:1, 2,7 42:1,8 43:21	destroy 81:10	directly 67:22 92:3,6 94:15	document 9:10 33:17 34:9
degrees 38:8,9 41:22	detail 14:15 19:6 72:25	disagree 42:12	documents 9:6,14 10:19
delays 85:5	details 23:24	discipline 16:25	dotted 65:17
deleted 80:16,23 81:5,15,20	determine 75:7	disclosed 98:7,25 99:2	download 34:15
deliberate 47:9	develop 26:5,9 41:6	disclosure 94:2	draft 99:17
demonstrate 31:18	developed 17:13 19:17	discrete 43:1	drive 48:21 86:15,16
denied 62:24	developing 24:11	discuss 8:3 14:14,16 36:7 41:12 42:25 43:1 46:25	drop 33:7 47:24
denies 63:18	developments 24:23	discussed 37:8 43:7 71:21 82:5 96:9	due 84:18 85:11
deny 59:7,23 66:2,12	deviations 47:8	discussing 18:11 21:7	duly 6:8
depend 85:21	device 27:21,23 28:8 48:20 49:23 56:4,23 83:4 86:12 87:10,18 90:7 93:15 94:13 95:13,20	discussion 36:11 99:23	duration 85:21
depending 68:4 77:14	devices 59:18 86:19,24,25 87:18	discussions 42:20	<hr/>
depends 53:14 60:10 68:3,20 71:19 75:10 80:3 84:25	difference 16:3,5 32:12,19 35:18	diskettes 48:20	E
depicted 92:12 93:7,11		disks 85:9	E2prom 87:8,14,15
deposed 8:25 10:24 11:6,11		disregard 48:2	earlier 27:15 37:8 41:25 43:14 66:17 69:16 96:9 99:7
			early 23:21 53:23 97:17
			easier

THE SULLIVAN GROUP OF COURT REPORTERS

Index: easily..Figure

<p>31:1 69:19</p> <p>easily 28:15</p> <p>echo 82:23</p> <p>edification 96:16</p> <p>edit 9:19</p> <p>editing 33:2</p> <p>education 23:3</p> <p>EE 38:25</p> <p>electrical 38:10,18,22</p> <p>electronic 14:3,21,24 22:3,7 27:21,22 28:1,8,18 38:4 50:13,14,20 54:7,15 83:4 94:13,16</p> <p>electronics 14:13</p> <p>elegant 95:18 96:6</p> <p>elements 29:6 44:10</p> <p>Ellison 45:20 86:2 87:17 88:12 89:1,12 94:2,6,18</p> <p>Ellison's 88:24</p> <p>embodiment 67:11,15 68:14,18 93:7</p> <p>embodiments 76:19</p> <p>EMV 55:8,13</p> <p>encapsulation 90:6</p> <p>encoded 61:4</p> <p>encrypted 56:5,23 57:1,5,10,14</p>	<p>58:19</p> <p>encryption 57:2,17,21 58:4 60:16, 23 65:1,7,10,12 67:4 93:3,4,8,11,14,16</p> <p>end 6:24 31:21 41:4 47:7</p> <p>engineer 88:25</p> <p>engineering 23:3 38:10,18,23 81:2 90:4</p> <p>enjoined 12:3</p> <p>entails 20:2,3</p> <p>entered 52:19 53:11</p> <p>environment 24:14,17 28:2,4,5,11, 14,15,18,25 29:12,15, 19,23 30:4,10,11,19 49:13 52:3 58:16,20,24 75:4 77:6 83:5,7 88:12, 17 92:19 94:21 95:13, 19</p> <p>environments 14:3,12,21,23 22:3,6 23:17 24:11,12 26:21 27:17 29:25 38:4 43:17 44:1 58:14 60:18 93:1 96:3</p> <p>equivalent 68:12</p> <p>error 10:8,16 33:2</p> <p>essential 18:2 40:7 67:5</p> <p>essentially 17:10 90:23 98:13</p> <p>EST 6:1</p> <p>establish 17:5</p> <p>Estonia 54:6</p>	<p>Europe 53:24,25 54:3 56:2</p> <p>evaluate 18:1</p> <p>evaluation 13:25 37:25</p> <p>evidence 25:22</p> <p>evolves 44:12</p> <p>EXAMINATION 6:12 91:19 97:16</p> <p>Excellent 91:17</p> <p>Excuse 46:10,15 88:3</p> <p>execute 28:22</p> <p>execution 14:3,12,20,23 22:3,6 23:17 24:11,17 26:20 27:17 28:1 29:12,14,25 30:3 38:3 43:17,25 48:16 88:12 89:17 90:20</p> <p>exhibit 9:15,24 10:10 33:8 34:24 35:3 48:22,23,25 49:4 86:3</p> <p>exhibits 9:3 22:24</p> <p>exist 38:8</p> <p>existing 51:7 74:19 95:20</p> <p>expect 39:9</p> <p>expensive 56:18 68:9 95:21</p> <p>experience 23:3 26:13 37:5 39:17, 20,24 40:1 41:10,15 42:5,6</p> <p>experienced 41:11</p>	<p>expert 7:5 13:4,23 18:23 20:16 39:8,10 40:16,19</p> <p>experts 41:14 70:17</p> <p>explain 15:4 50:25 59:9 62:6 96:15</p> <p>exposes 52:23</p> <p>external 73:12,14 74:2 80:4,8, 15,22,23,24 81:4,6,15, 20 82:2,9</p> <hr/> <p style="text-align: center;">F</p> <p>facilitate 36:11</p> <p>fact 32:25 41:14 51:10</p> <p>factors 70:6</p> <p>fair 69:20 90:22</p> <p>family 44:19</p> <p>Fantastic 7:2 9:13,22</p> <p>feasible 89:4</p> <p>feel 78:14</p> <p>field 14:19 25:9</p> <p>Figure 58:15 59:22 60:12,20 64:13,16,19,23,25 65:13,18,24 67:11 68:1, 2,8,15,16,18,22,24 69:2 71:4,9 72:19 73:23 74:10,12 75:18,21,22, 25 76:5,18,19 77:4,13 86:6,11,15 87:20 88:10, 19,20 90:19 92:12,13, 14,18,24 93:1,8,12 98:14</p>
---	---	---	---

THE SULLIVAN GROUP OF COURT REPORTERS

Index: file..histories

file 22:24 33:8,9 34:4,23 65:22 filed 24:1 31:17 33:14,19,20 34:9 44:14 files 33:10 filing 44:16,20 52:14 fill 98:21 financial 55:18 56:12 find 9:9 98:3,22 fine 7:25 9:17 10:1 36:14,17 45:2 48:6 70:25 71:1 83:2 91:12,13 Fish 6:22 7:4 fit 19:6,19 fitting 43:4 five- 44:25 flash 87:13,14 flaws 70:5 flexibility 76:15 floppy 48:20 86:15 focus 14:19 focused 38:19 focuses 96:4 follow-up 97:15	force 77:10 form 25:4 57:1 63:20,23 65:12 94:4 97:5 format 9:7,9 20:5 57:14 forming 22:22 25:2 forms 64:23 formulation 78:18 forward 33:17 34:8 50:20 58:11, 12,13 93:12 95:3 found 98:7 framework 24:24 fraudulent 95:16 free 78:14 Friday 36:9,13 front 9:11,25 10:1 22:20 23:20 32:22,25 33:9,10 34:5 50:9 71:6 83:2 86:4 fully 11:24 14:18 15:19 17:25 18:5,20 19:12 20:23 21:18,21 25:25 30:8 74:17 function 59:10 60:8,9 62:13 87:25 functionalities 89:16 90:18 functionality 31:1 70:17 functions 15:11,13 60:8 65:2 75:12 90:1,16 91:6	fundamental 94:22 <hr/> G gave 63:16 64:20 general 7:13 18:23 19:2,4 25:8, 10,16 26:9,25 28:15 29:16 38:21 39:2,3,11 89:1 generally 29:14 80:7 generated 54:21,23 give 9:10 17:15,22 33:25 59:21 61:23 62:2 65:3 68:10 69:11 85:2 giving 62:5 goal 15:16 49:10,12,17 goals 16:11 87:25 good 6:13 91:9 Great 6:21 8:1 9:18 10:2 33:25 34:17 36:18 45:5 71:8 greater 90:17 group 27:8 guess 6:17 20:21 23:14 36:10 44:11,14 58:1 87:2 <hr/> H half 55:10 hand 28:18,23 29:17,18,19 49:3 53:8 58:14 75:3,4	handled 62:25 happen 69:2 81:7 happened 24:23 happening 26:10 39:3 hard 48:21 56:13 85:9 86:16 89:3 hardware 14:2,11,20 22:8 26:19 27:11,14 30:8 38:3,25 50:15 51:2,5,11,12,15, 17,18 52:4,19,22 67:12, 13,14,19,21,24 68:8 72:20,22 73:5,24 75:17, 19 76:1,9,13,18 92:19, 21 93:1 95:21,24 96:25 hash 15:11,13 header 10:14 hear 65:9 hearing 82:22 helps 22:14 42:14 93:22 Henry 7:1,6,9 20:4,9 33:24 45:3,4 71:1 91:13,16, 17,19 92:10 94:6,9,23 97:12 99:5,24 hide 77:22 high 39:13 higher 68:10 highly 69:18 70:16 hindsight 26:11 histories
---	--	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: hope..issue

22:24	implementations 26:19 73:25 82:14 87:6	84:12,13 87:9,11	interaction 16:10 42:9
hope 22:14	implemented 54:16 62:9 91:4 92:19	initially 24:3	interface 59:6 89:17,20 90:21 91:25 92:16
host-to-peripheral 89:17,19	implementing 96:25	innovative 18:18	internal 73:12
hour 44:25	important 15:6,17 17:6 27:19 28:12 76:20 96:17,18	input 30:24 97:10	international 11:1,11 24:5
house 24:9	impossible 98:4	input/output 59:11 87:21	Internet 54:9,14,17
housing 91:5	inaccessibility 30:3	insecure 58:5 61:17,18 63:10	interpretation 32:5 35:12
Houston 34:14 45:7	inaccessible 27:24 60:2 65:25 66:4 94:13,14,15	inside 28:2 52:2 53:4 58:25 73:7 74:7 79:15 91:5	interruption 81:23
hub 87:21 88:21	include 26:13 27:11,13 37:25 42:23 50:4 61:17 63:14 76:5	insights 17:15	interventions 50:19
hundreds 85:5	includes 10:8 20:20 49:22,25 53:17 60:23 79:23 86:15,18,21,22 88:4	inspected 79:13	invention 44:14 55:18 67:6 76:19
<hr/> I	including 13:24 14:1,10 38:1 52:20 54:3 71:9	inspection 77:20 97:7	inventor 11:17
I/o 83:24 86:18,25 87:17 90:1	incorporate 90:18	institute 31:15 35:5	invoke 92:23
ICH 87:20,23 88:4 89:5,24 90:13,16,18	incredibly 89:2	institution 56:12	involved 11:15,21 12:11 13:11 23:22 24:2
ICHS 88:24	independent 28:11 77:9	institutions 12:4	involves 26:20 83:22
idea 58:13	indicating 20:14	instruction 80:2	IP-RELATED 13:5,7,10,14
ideally 38:13	indication 35:24	instructions 69:9 79:21,23	IPR 11:21 12:3,6,20 32:4, 11,13,18,20 33:12 35:11,19,22,23 36:2,5
ideas 43:17 96:1	industry 23:5 24:23 26:18 27:2,8 39:17 41:9,16	integrate 90:7	IPRS 12:8
identification 50:14	inform 42:10,13	integrated 89:5,15,24 90:14	isolate 51:6
identity 54:7	informal 87:15	integrates 89:16	isolated 88:11,16 89:16 90:19
immediately 84:6	information 31:16,18 52:24 57:11	intellectual 12:21 13:12	isolation 96:7
implement 15:15 23:17 30:8 61:25 62:3,14 69:15 76:7 98:11		intention 47:11	issue 51:22 78:3
implementation 12:18		inter 12:21	
		interact 41:15,16	

THE SULLIVAN GROUP OF COURT REPORTERS

Index: issued..making

issued 54:6 56:11 issues 13:12 ivory 41:13 <hr/> <p style="text-align: center;">J</p> Jacob 6:15,23 7:6 Jeremy 6:22 7:4 job 70:8 joined 6:21 June 44:16 55:21 56:6 junior 41:11 <hr/> <p style="text-align: center;">K</p> K-E-R-C-K-H-O-F-F-S 96:19 keeping 24:21 Kerckhoffs 96:20 Kerckhoffs' 96:19 key 16:9 24:11 27:22 29:3 53:18,21 54:21 55:3,11, 12,22 56:8,11,22,25 57:7,9,13,18 58:17,19 60:16,23 65:1,7,10,12 69:13 93:3,4,9,11,14, 16,19,23 94:12 96:24 97:2,9 keys 43:18 51:5,19 53:3,4,9 55:16,17 56:4 58:23 64:6 67:13 69:15 77:1 93:3,9,17,22 94:19 Khan 6:12,15,16,23 7:2,3,10,	11,17,19 12:9 15:1 16:2 19:22 20:7,11,17 22:15 25:1,20 29:8 33:25 34:2,14,17,18 37:16,18 44:3,24 45:3,5,10 47:16 49:15 52:5 54:10 64:12 68:13 70:22 71:3 73:9 75:6 78:10 81:24 82:12, 20,21 83:16 85:16 86:1 88:15 89:22 91:8,15 94:3,7 97:14,16 99:12, 17,21 kilobytes 85:15 kind 41:6,13 52:11 knowledge 23:3 25:11 37:3 <hr/> <p style="text-align: center;">L</p> language 20:15 languages 83:23 large 12:5 23:15 85:6 larger 17:5 84:9 90:6 late 24:21 26:16 53:24 latency 85:23 Latin 24:17 layer 30:5,13,16 lead 95:16 learn 26:11 leave 80:20 left 57:15 legitimate 50:21	level 30:15 39:13 41:1 42:5, 14 43:24 68:3,6,10,20 limit 21:23 67:18 limitations 15:18 limited 22:1,2 36:15 43:3 90:24 lines 36:10 61:2,3 65:17 67:3 83:8,21 89:12 list 10:15 21:6 23:19,20 listed 37:24 listening 6:24 liter- 23:16 literature 23:16,23 24:13,22 25:11,14,16 26:8 live 54:6 load 80:13,14,19 loaded 48:16,19 71:15,18 72:8, 13 82:6,7 loader 48:17 88:5,7,8,11 loading 50:1 79:25 located 88:11 location 29:1 65:21 67:4,10 84:11,22 99:1 locations 66:7 log 65:22 logical 90:20	login 57:10 long 11:9 84:24 longer 70:18 80:19 81:6,8,9 loses 87:10 lot 12:3 26:12 41:16 LSM 15:10 <hr/> <p style="text-align: center;">M</p> MAC 53:17 55:1,16 machine 95:23,25 made 8:25 75:5 78:12 92:1 95:1 97:6 98:4 magic 84:5 magnitude 85:13 mail 47:22 main 85:3 major 95:2,3,7 majority 56:10 make 9:20 19:20 30:1 31:1 33:6,16 36:8,9 46:7 47:3,11 51:3 60:6 64:1 68:7,19 69:10,19 76:22 77:10 81:11 92:20 93:12 makes 31:1 63:2 69:19 81:1 93:14 95:19 making 89:2
--	---	---	---

THE SULLIVAN GROUP OF COURT REPORTERS

Index: malware..nub

malware 95:14	16	message 55:1	Muir 45:20
manage 92:8	MCHS 88:23	method 50:12 96:21	multiple 11:8 31:4 61:21 69:3 88:23,24 89:16 90:6
management 24:12	means 21:20 44:11 62:10 65:15,17 77:19 78:22 84:4,5	methods 51:7,9	<hr/>
manager 90:20	meant 13:7 20:13 61:9 95:13	milliseconds 85:14	N
manages 91:23	mechanism 73:21	minimal 70:17	names 9:15
manipulate 58:23	mechanisms 74:6	minus 40:14	nanoseconds 85:5
manner 8:8	mediate 59:17	minutes 7:21 45:6 91:10	necessarily 18:7 82:4
mark 91:9	mediated 67:17	missing 26:3 42:16	needed 39:21 42:3,15 61:14 62:14,15 74:8 75:10
mass 48:19 86:12	mediates 67:25	misunderstood 32:15 46:10	network 26:17,24 27:5 59:18 62:11
master 14:17 17:7 37:6 39:25 41:1,3,4	memories 84:9	mix 44:21	newer 66:24
master's 37:12,23 38:18 39:20 43:21	memory 27:21 28:3,25 30:9 51:17 57:1,14 58:6 59:8,17,20 62:12 63:1 65:18 66:1,4,7 71:20,25 73:1,3,4,10 74:15,18,24 75:2,7 79:17 80:4,6,8, 11,12,15,16,22,23,25 81:4,6,15,20 82:1,2,3,7, 9,10,11,18 84:7,10,14, 15,17,22 85:3,5,19,20, 23 86:22 87:4,6,7,8,11, 12,13,16 88:20 89:20 90:12,17 98:18	mode 89:17	nice 47:21
mastered 17:2	mention 22:22 23:2,8 32:3,10, 11,17 36:19 41:18,20, 25	model 55:4	nonsecure 75:9
material 27:10 93:23	mentioned 12:15 14:9 15:3 20:12 26:12,14 27:15,16 38:19 42:2 43:13 52:6 54:24 56:7 57:9 58:10 60:7 66:14,17 69:16 78:15 88:16 95:9 97:17	modification 73:17	nonvolatile 73:1,3,4,10 82:6,10 86:22 87:4,5,7,8,12
mathematical 16:7		modify 67:12 76:7	normal 57:23
mathematics 43:2		modifying 51:8 68:8	note 37:22
matter 11:12 13:24 15:3 17:11 19:3,5,11,13,24 20:1,6, 13,16,24,25 21:5,12,16, 17 23:9 26:14 29:5 37:3,7,13,24 38:7 39:15 42:23 78:4 97:4		Module 24:5	noted 37:13 40:17 90:19
matters 11:16 12:12 38:11 39:2 41:12		modules 24:8 43:16 48:19	notes 34:7
mature 41:5	merchant 53:8	moment 39:8 43:20	notions 38:11 39:12
MCH 88:20 89:5,15,25 90:12,		Monaldo 6:22 7:4	novelty 66:15,18
		morning 6:13	November 6:1
		move 33:16 36:5	nub 48:16 86:22
		moving 34:8	

THE SULLIVAN GROUP OF COURT REPORTERS

Index: nub/executive..perform

nub/executive 88:4,11 number 10:7,8,15 49:3 55:6 96:11 numbers 9:15 NVM 73:3 <hr/> O oath 8:14,16,17 objection 20:4 33:22 94:3 occur 55:23 occurred 32:24 official 99:19 one-hour 91:9 online 95:9,11 open 34:4,5 50:7 70:5 86:2 operate 39:4 operates 19:15 operating 27:24 28:9,11,12,13,23 29:2,19,21,22,24 30:1, 6,13,16,18,20,22 31:4,8 52:22,25 57:24 58:15, 21 59:1,3,8,19 60:3,9 61:10,11,14,19 62:8,23 63:3,17,18 65:19 66:3, 5,9,11,20 67:15,23 68:25 69:3,5,17,18,21, 22 70:1,3,14,16,18,20 71:22 72:1,4,16 74:22 75:3,13 77:21,22,24 78:8,16,21,23 79:11,14 83:4,7,24 94:14 95:15	operation 16:7 59:16 60:17,18 62:8 87:23 90:25 91:2 operations 83:25 84:20 operator 71:20 opinion 14:7 34:23 37:21 50:18 89:1 opinions 22:23 25:2,4 26:5 35:16 47:7 opponent 68:7 option 76:3,17,18 options 54:25 90:8 95:24 99:21 order 16:19 76:10 85:4,11,12 ordinary 36:21,25 37:11,22 38:17 39:15,21 40:3,14, 19,20 42:11 73:22 95:23,25 organization 24:6 original 12:16 OS 70:8,10,11 98:15 OSS 70:11 outcome 57:17 outset 36:7 overcome 45:18 overlapping 18:18 owner 7:6 9:1,4 45:23 46:5,11, 13,20 47:5,17 48:10	owner's 7:5 45:12,19 48:12 oxymoron 70:10 <hr/> P pages 10:15 paragraph 12:24,25 13:2,18,22 19:23 20:6,15 22:17,22 23:7 27:16 31:11,14,22 32:2,10,11,16,17 35:4, 10 36:19 37:13,22,25 45:14,17 48:15,23 49:1, 6,9,16,19,22,25 50:11 51:10 58:8,9,10 83:17, 20 paragraphs 22:18 32:3 50:3 paraphrasing 94:25 part 41:20,21 46:20 61:5,7, 9,17,18,22,23,24 62:5, 12,18,19,20,22 63:2,3, 5,6,9,10,11,13,16,17, 20,21,24 64:2,6,17,20, 23,25 65:5,13,18,24 66:23,24 71:20 72:22 74:1,23 75:2 79:18 83:24 98:17 part's 63:7 partes 12:21 participating 6:24 parties 16:10,14 partners 12:5 parts 60:14 61:13,24 62:2,3 65:4,11 pass 97:13	passage 98:3 passing 66:10 password 56:5,24 57:3,10 past 26:22 patent 7:5,6 9:1,4 10:4,7,8,9, 15,25 11:15,20 12:12 14:7,14,18,19 15:5,10, 16,19,20,22 16:23 17:2, 3,23,24 18:11,12,17,24, 25 19:14,15 20:8 21:19 22:1,23,24 24:1 27:19, 25 28:6 32:3,8,18,25 35:10 36:12,13 37:4,9 42:24 43:7,25 44:15,16, 19 45:12,19,23 46:5,11, 13,20 47:5,17 48:9,11 50:8,12,19 51:1 52:15 53:16 54:16 58:10 60:12,20 61:1 62:17 63:12 65:15 66:18 68:23 71:18 91:21 93:5, 8,10,11 94:1,18 95:2 97:22 98:7 patent-related 11:12 13:16 patents 9:11 11:17 12:16,17,18 27:20 29:7 42:25 pause 50:6 70:22 payment 52:20 payments 55:8 PC 24:8 43:14 56:14 57:19 people 40:23 41:9,10,11,12,15, 16 42:4 43:11,23 51:20 52:19 95:9 96:1 perform 17:6 51:19 58:4 61:15 90:1,23
---	---	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: performance..processor

performance 90:10	phrase 20:1	position 18:25 19:9 25:21 37:10 38:16 70:14 79:9 98:24	prevents 59:1,3
performed 57:22 95:12	physical 95:10	possibility 98:8	previous 54:24
performing 50:13 52:1 90:16	pick 35:1	possibly 16:8 96:10	previously 94:24 98:12
period 23:25	Picking 71:4	post-grant 12:11 31:16 32:10,14, 17 35:6,20	principals 23:4
periodic 7:14	piece 30:7 69:12 71:24 91:22	potential 52:6,7	principle 73:16 93:18 96:18,19
permanent 82:3,18,19	pieces 61:21	potentially 51:5	printed 9:7 47:19
permission 63:4,8,11	place 22:4,7 28:5 62:16 84:18 91:9 92:23 98:3	power 87:10	printer 62:11
permit 59:25	places 59:7 75:22	practice 60:9 80:20 91:3,4	printers 59:18 87:2
person 36:21,25 37:10,21,23 38:13,16 39:9,15,21 40:3,14,20 42:11 43:20, 22 73:22	plain 15:22	practices 23:4	printout 34:6
perspective 36:21 40:13,18 41:21 42:10 43:10	planning 36:11	precise 62:4 68:15 88:3	prior 93:13 95:3,7,8
petition 31:16,17,20 35:6,21 36:1	platform 24:3,5 43:16 56:14	preexisted 93:9	private 27:22 29:2 54:21 55:11, 22 56:4,8,10,22,25 57:7,9,13,18 94:12
Petitioner 22:25	played 13:13	prefer 33:21,24	problem 32:24 56:12
petitioner's 7:3 46:12	plays 98:16	preferably 70:7	problems 43:25
PGR 32:13,20,22 33:1,4,12 35:19 36:5	point 8:7 66:15,17 76:20 81:2 97:22 98:2 99:1	Preneel 6:7,14,19 7:5,12 20:11 34:3 45:11 47:18 49:16 71:5 82:25 83:18 91:20 97:17	procedure 10:25 12:14 35:22,23 36:2
PGR' 35:6	pointed 98:10	preparation 10:19,22	procedures 12:13
phase 35:21	points 66:15	prepare 59:15	proceedings 6:25 8:22 9:24 11:22
Phd 24:6 37:6,12,23 38:18 39:20,25 40:1,8,11 43:21 44:4,5	portion 15:22	present 6:3 7:1 67:6	process 57:17 81:8
Phds 41:10	ports 59:18,20 87:3	presented 31:17	processed 79:15
phonetic 43:2	POSITA 41:21 43:11,22,24 44:11	prevented 69:23	processing 49:13 90:20
	POSITA's 44:9	preventing 68:25	processor 48:16 57:23 63:1 73:5, 7,8,11,13,14 74:2,3,7,8 82:16 84:8 85:22 86:22

THE SULLIVAN GROUP OF COURT REPORTERS

Index: processors..regulates

<p>88:4,10</p> <p>processors 51:4 73:6</p> <p>producing 12:3</p> <p>program 59:14 79:20,21,22</p> <p>programming 83:23 91:25</p> <p>programs 39:18</p> <p>projected 47:22</p> <p>projects 12:3,5,6,7</p> <p>pronouncing 6:18</p> <p>proof 39:12</p> <p>proofs 14:2,11,16 16:23 17:7, 10,21,23,25 18:3,7,13, 20,22 19:2,7,10,16,21 22:12 38:2 39:10</p> <p>properties 89:10 90:10</p> <p>property 12:21 13:12</p> <p>proprietary 56:1 78:5</p> <p>protect 49:13 53:10 93:22 94:16,20</p> <p>protected 28:2 57:14,16 69:4 73:15,17,19 77:6 78:6</p> <p>protection 73:18 74:4,5,8 96:8 97:2</p> <p>protector 48:15 49:10,12,17 50:1</p> <p>protects 72:16</p> <p>protocol 16:9 53:5,6,7</p>	<p>protocols 14:1,10,15 15:9 16:4, 12,15 17:1,14,20 22:10 37:14 38:1 56:1,7,9</p> <p>prove 18:3</p> <p>provide 23:24 25:8 95:25</p> <p>provided 52:2,19 53:7 56:15 94:12 95:24 97:8</p> <p>providing 7:14 26:18 51:4 95:12, 18</p> <p>public 53:21 54:21 55:12 77:10,19,23 78:4,7,15, 25 79:1 96:12,16,24 97:1,6</p> <p>publication 23:8,12 25:24</p> <p>publications 23:14,18 24:7 25:3,4,7, 8</p> <p>publicly 96:22 97:7</p> <p>put 24:19</p> <hr/> <p>Q</p> <p>question 12:10 18:10,17 19:8,12 20:5,7,10,18,20 25:25 26:2 29:9,11 32:15,16, 19 36:1 37:20 46:10 63:23 64:1,3,21,22 74:17 75:20 78:9 81:3 87:24 94:8,10</p> <p>questioning 7:22 19:24 36:12</p> <p>questions 7:13 10:21 11:20 12:20 21:11 34:11,20 36:15 91:15,18 94:5 97:13,15 99:5,13</p> <p>quick 97:14</p>	<p>quote 36:20</p> <p>quotes 31:21</p> <p>quoting 20:14</p> <hr/> <p>R</p> <p>RAM 71:24 72:4,7,14 74:12, 19 82:7,10 84:7 92:25</p> <p>random 71:24</p> <p>read 13:2 14:5 20:7 23:14 31:14 45:23 46:1,3,15 49:9 53:22 61:2,4,10, 11,13 62:21,22,23 63:4, 17,19 66:10 67:3 69:14 80:12 84:9,14 85:3,6,9, 17 89:13,23</p> <p>read/data 83:22</p> <p>read/write 84:19</p> <p>reading 31:22 78:12 84:10,17 85:18</p> <p>reads 48:15 85:24</p> <p>real-life 43:5</p> <p>realm 98:8</p> <p>reasonable 32:4 35:11</p> <p>rebutted 31:18</p> <p>recall 69:11</p> <p>receiving 30:24</p> <p>recent 26:9</p> <p>recently 24:1,10</p>	<p>recess 45:9 71:2 91:14</p> <p>recipient 55:3</p> <p>recite 83:12</p> <p>recites 83:4</p> <p>recollection 99:10</p> <p>reconvene 45:5</p> <p>record 6:25 26:6 31:14 99:16, 22,23</p> <p>recovery 65:20</p> <p>redirect 91:16 94:4 97:12,18 99:4,6</p> <p>reductions 14:1,11,16 16:22 17:7, 9,21,23,25 18:3,7,20,21 19:1,7,10,20 22:11 38:2</p> <p>refer 9:14 25:6</p> <p>reference 26:3 86:3</p> <p>referred 25:7</p> <p>referring 10:9 23:12 34:9 44:5 51:1 57:19 58:14 62:18, 20 79:17</p> <p>refers 51:10 88:9</p> <p>regular 30:11 41:8 52:21,22 57:23 74:22 75:13 94:21</p> <p>regulate 62:15</p> <p>regulated 59:6</p> <p>regulates 61:22 66:13</p>
---	---	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: related..Searle

related 13:11 14:8 15:10 17:11 21:7,8,11 43:25 relating 45:19 relative 84:19,25 relevance 17:18 20:14 relevant 13:24 15:3,5 16:23 18:23 20:16,25 21:5,12, 16 23:9 27:18 relied 23:2,8 25:22 rely 96:23 relying 25:2,3 remain 80:9,14 96:21 remains 81:19 92:23 remember 37:1 remotely 6:4 remove 80:23 removed 80:7 renamed 24:4 rendering 60:2 repeat 18:15 19:8 29:10 32:16 37:19 41:19 52:9 86:7 92:5 repeated 39:13 rephrase 64:22 replace 70:1	reporter 6:5 12:1 14:22 15:12 19:18 22:5 24:15 25:13, 16,19 28:20 34:16 37:15,17 45:8 47:15 49:11 51:24 54:4 64:10 68:5 73:2 74:25 78:1 82:8 85:8,25 88:14 89:18 92:4 99:15,20,22, 24 represented 50:19 58:11 request 7:16,20 35:22 69:12 requested 12:1 14:22 15:12 19:18 22:5 24:15 25:13 28:20 37:15 47:15 49:11 51:24 54:4 64:10 68:5 69:10 73:2 74:25 78:1 82:8 85:8,25 88:14 89:18 92:4 requests 99:16 require 76:12 required 17:20 21:11 28:5 29:11, 14 requirements 89:8 requires 66:11 68:8 requiring 50:15 51:2 research 11:25 12:2 researcher 24:20 resistant 68:19 respect 67:5 respectfully 42:12 respective 22:24	response 9:1,5 45:19,24 46:5,11, 12,13,21 47:5,18 48:10, 12 rest 10:15 restrict 59:25 97:19 restricted 22:2 30:25 66:8 restricts 66:4 result 18:4 72:13 results 43:5 retail 56:15,19,21 retrieval 83:22 review 10:18 12:21 31:16 32:7, 11,15,17 35:6,20 45:23 reviewed 22:23 reviewer 53:22 rewritten 61:13 87:10 rhetorical 78:3 Richardson 6:22 7:4 rights 12:21 Ring-0 88:13 role 13:13 67:19 98:16 rolled 53:24 55:13 ROM 61:12 73:11 74:1 80:11 82:14,18,19	rough 99:17 run 30:19,20,23 58:16 59:14 72:1 73:6 77:25 78:21,23 79:13 92:22 run-time 83:5 running 12:5,7 69:9 71:23 83:6 runs 69:10 92:25 93:1 <hr/> S S-A-N-C-U-S 24:16 Sancus 24:13,16 scenario 56:20 57:19 90:14 scheduled 36:9 scheme 15:9 schemes 15:14,15 18:14 22:13 science 16:14 19:16 38:9,12,22 39:1 scientific 21:18 24:22 43:5,15 scope 21:1,20,25 27:25 39:17 94:4 Scott 7:1,6 scratch 40:15 57:7 66:16 88:18 screen 48:4,7,9 screens 87:2 Searle 45:18
---	---	---	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: secrecy..software-only

secrecy 96:23 secret 55:3 76:21,23 77:2,3,5, 7,11,14,17,19 78:3,5 97:2,9 Section 31:17 sector 53:19,21 secure 14:2,3,12,20,21,23,24 15:9,15 16:11 17:24 18:4 22:3,7 23:17,22,23 24:11,17 26:19,20 27:17,22,24 28:1,2,4,5, 11,14,18,24,25 29:2,3, 4,11,14,23,25 30:3,10, 19 31:2 38:3,4 43:17,25 44:1 49:13 51:3,5 52:3, 7,8,12,16 53:7,9,12 55:22,23 56:3,8 58:2, 15,16,17,18,20,24 59:2, 25 60:2,17 61:5,9,10,17 62:17,19,20,22,24,25 63:1,2,5,6,7,10,13,16, 20,24 64:2,5,14,17,20, 23,25 65:4,5,13,16,18, 20,25 66:12,13,19,24 67:1,4,10,12 68:1,15, 23,24 69:4,7,9,19,22,23 71:9,13,17,18 73:21 74:9,18,23 75:4,8,11,16 76:6 77:18 78:6,25 79:15 80:1,17 81:14 91:24 92:9,15,25 93:17, 23 94:12,20 95:12,19, 23,25 96:2,3,13,16,21 97:9,10 98:17 securing 52:1 security 14:1,10,16 16:11,15,20, 22 17:6,9,21,23,25 18:1,2,13,14,19,21 19:1,7,10,15,20 21:22 22:11,12 24:7,9 26:17, 19,24 27:5 38:2,14 39:10,12 43:15,19 68:10 89:8 90:9 96:22 send 33:19,20,21 34:1 69:9	sender 55:3 sense 21:14 81:1 97:4 sentence 15:2 18:15 21:15 23:7, 13 31:24 61:8 67:3 separate 30:9 51:17 67:14 71:20, 25 83:7 89:25 90:5 91:3,4 94:20 separately 90:13 separates 30:6,17 separation 28:17 29:17 66:19 separator 98:16 series 84:6 serve 95:2 served 11:2 13:4 server 53:8 session 11:9 set 62:10 93:4 setting 53:14 settings 55:7 69:15 share 48:4 55:3 shared 55:17 sharing 49:8 short 91:10 shortcomings 21:22	show 47:21 shown 48:9 65:24 76:5 86:14 shows 42:13 71:9 88:10,20 96:4 sic 46:16 side 7:3,5 29:18 53:12 sides 15:24 16:6,16 18:5 sign 55:11 signature 55:15,16 signatures 53:13,15,18,20 54:1,8, 9,13,19,22 55:10 signer 55:2 significant 50:20 58:11,12 signs 14:17 similar 43:16 81:9 Similarly 89:24 simple 70:7,8,10,12 91:22 95:18 96:6 simpler 75:11 95:24 simplified 30:18 69:18 simply 79:17 single 50:4 90:7 sir 99:25 sit 30:15	sitting 41:13 92:15 situated 18:24 size 27:9 75:10 sizes 85:1 skill 36:21,25 37:11,22 38:17 39:16,21 40:3,14, 19,20 42:11 73:22 skills 18:22 41:7 slightly 41:2 slowly 92:5 smaller 75:12 smart 23:22,23 51:21,23 52:2, 3,4 56:11,13,17 57:20 58:25 81:10 software 14:2,12,20 22:8 27:12, 14,23 28:22 29:4,6,20, 21,22 30:7 38:3 51:6 52:6,7,11,16,19 57:24, 25 58:18,24 61:22 64:8, 11,14,17 65:20,23 66:25 67:13,16 69:9 71:10,12,17,23 72:1,3, 19 73:6,16,19,20 74:3, 11,14,16 75:16,19,24 76:6,8,10,16,21,24,25 77:1,2,5,14 78:3,20,24 79:10,12,16,19,20,22 80:1,7,13,17,21,24 81:4,5,13,19,25 82:3,6 83:6 91:22 92:15,17,18, 22,24,25 93:19,20 95:22 96:10,12,25 97:2, 5,6,11 software-based 56:3 software-only 51:9
--	---	---	---

THE SULLIVAN GROUP OF COURT REPORTERS

Index: softwares..table

softwares 73:24 solemn 8:17 solution 96:7 97:8 solutions 56:3,14 72:24 sort 30:1 83:23 sorted 36:2 sound 36:13 70:23 source 84:14 space 48:16 74:15,18,19,22 75:12 82:1,4 spaces 75:8 79:18 80:6 speaks 49:16 69:21 special 51:18 specific 12:17 16:11 17:2 18:10 22:14 26:18 27:8 37:3 42:4 43:24 61:25 62:4 69:13 92:1 93:6,15 98:2,10 specifically 19:5 21:23 25:11 53:15 55:21 62:1 72:25 74:6 88:1,12 93:3 94:1 specification 21:8 specifications 53:22 55:8,9 specifics 7:13 speed 84:19 85:22 speeds 84:10,25 85:3,23	split 60:5 SSL 53:5 stage 9:21 43:22 standard 31:25 32:7 35:15 73:18, 20 74:3 78:4,5,7 97:8 standards 17:19 stands 59:10 start 6:17 7:12 13:22 28:7 65:3 started 9:19 65:3 87:3 starts 59:12,14 startup 60:8 72:10 state 35:10 44:11 45:17 50:11 statement 13:7 20:12 21:4 24:19 33:1 49:22 58:9 83:20 90:2,22 statements 8:25 78:12 states 10:3 31:15 35:5 48:19 50:18 96:20 stays 87:11 step 58:13 93:12 95:2 steps 50:20 58:11,12 95:3,7 stipulate 6:3 stop 7:23 35:7 49:8 stopped	79:13 storage 48:19 49:23 58:17,18 65:21 67:4,10,13 85:21 86:12 store 51:18 75:15 76:17,18 80:1 84:20 85:13,19 87:9 stored 48:19 56:4,11,22 57:1, 6,13 61:4 63:1 64:8,15, 19 65:1,25 71:13,14,15, 17 72:3,14,23 74:7,11, 13 75:19 76:15 80:5,24 81:13,18,25 82:3,10,14 84:13 stores 81:4 storing 27:21 story 66:23 strengths 15:18 string 16:7,8 93:19 stripped-down 70:16 student 24:7 43:14 students 27:6,7 40:25 41:2,4,22 42:6,10,17 43:8 studied 21:19 studies 16:14 study 16:25 17:14,16 18:8 19:5 subject 13:23 15:3 17:11 19:3, 4,11,13,23 20:1,3,6,13, 16,24 21:4,12,16 26:14 37:3,7,12,24 39:1 42:23 93:3	submitted 9:1 22:25 subsequent 8:21 12:20 subsequently 76:7 substance 8:3 20:4 sufficient 38:6 39:15 42:7 summarize 78:13 supervise 41:3 support 9:1 26:5 56:19 98:22 sworn 6:4,8 8:14 symmetric 53:18 54:25 system 16:20 17:5 18:4,6,8,19 19:14 27:24 28:9,12,13, 23 29:2,19,21,22 30:1, 6,13,16,18,20,23 31:9 50:13 52:22,25 57:24 58:15,21 59:1,4,8,11, 12,17,19 60:3,11 61:10, 11,14,15,19,24 62:3,8, 9,23 63:3,17,18 65:19 66:3,5,9,11,20 67:4,5,9, 15,23 68:1,25 69:2,17, 18,21 70:1,6,15,16,18, 20 71:22 72:1,4,17 74:22 75:3,13,15 76:2, 5,8 77:21,23,24 78:9, 16,21,23 79:11,14 83:5 86:14,18 87:17 88:19, 24 94:14 95:15 98:11 systems 16:1 28:6 29:24 31:5 39:4 43:3,5 68:12 69:3, 5,22 70:3,4 83:24 <hr/> T <hr/> table 59:6 61:4
---	---	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: talk..understand

talk 44:21 talking 30:2 41:14 42:17 52:13 Tamara 7:17 tangentially 17:11 task 70:20 tasks 70:11 taught 26:23 TCPA 24:24 teach 40:23 41:1 teaching 26:13,16,25 27:8 technical 13:23 20:15 21:17 41:10,12 47:7 59:13 65:2 technically 89:3 techniques 17:1,3,8 21:21 73:18,20 technologies 55:18 technology 21:19 23:9 50:21 53:21, 23 telling 29:12 temporarily 84:21 temporary 82:11,18 ten 24:18 45:6 91:10 ten-minute 45:1 70:23 tend 42:25	term 20:18,19,22 55:13 78:22 96:12 terms 36:20 59:13 testified 6:10 testifying 8:18 testimony 8:4,10,13,14,21 96:9 thesis 41:3 44:4,5 thing 66:24 things 19:17 26:11,20 39:11 43:4 56:1 85:13 90:3 thinking 51:21 52:1 thinks 40:20 thoughts 43:10 threat 68:3,6,20 time 7:16,21,22 11:8,9 44:12,13,14 47:25 52:15,17 53:2,13,23 55:17,20 72:8,9,10,11 80:14,19 81:7,11 86:9 87:3 89:10 97:24 98:1 times 11:2,8 32:14 timing 44:9 TLS 53:6 today 8:4,13,17,21,25 10:19 17:18,19 18:1 36:12,15 55:6 token 90:21	told 10:23 toolboxes 17:13 tools 17:1 21:18 top 28:9 topic 23:16 24:20 27:2 96:10 topics 14:8 38:19 41:6,13 tower 41:14 TPCA 24:3 TPM 24:3,4,24 TPMS 24:8 43:15 traffic 61:22 train 41:15 training 42:5 trainings 26:18 transaction 16:12 28:2 29:3,4 50:13,20 51:6,23 52:8, 12,20,24 53:11 55:11, 12 94:16,17 97:3 transactions 14:4,13,21,24 15:15 22:4,7 28:16 38:4 44:1, 2 49:14 51:4 52:1,16,17 54:9,15 55:6,19,23 56:10,17,22 64:7 65:22 67:1 92:2,18 95:9,10, 11,16,17,23,25 96:5 transcript 99:15,19 transcription 78:13	transfer 84:6 transferred 53:12 84:13 transform 16:8 trial 8:18,21 true 86:18 trusted 24:3,5,8 28:16 43:16 truth 6:9,10 10:23 Tuesday 6:1 turn 9:23 12:25 45:14 49:6 60:25 67:2 82:22,24 86:5 89:11 93:2 turning 31:11 48:14 71:4 83:17 types 86:24 typical 70:20 85:11 typically 16:13 26:20 27:8 29:18 30:5,12,25 37:4 38:10, 23 39:1 52:11 55:5,7 56:5 61:12 69:8 70:3,11 75:11 84:9 86:24 87:5,8 93:21 typo 10:12 32:21 typographical 10:8,16 <hr/> U unable 98:22 undergraduate 41:22 understand 8:2,6,13,15,16,19,20, 23,24 9:2 11:24 14:18
--	--	--	--

THE SULLIVAN GROUP OF COURT REPORTERS

Index: understanding..young

<p>15:7,8,18,19,22 16:20 18:1,2,8,13,20,21 19:12,14,16 20:21,23 21:2,3,18,21,25 22:12, 13 25:25 29:12 31:15 33:5 35:5 37:7,9 38:11, 25 40:13,18,21,25 41:5, 20 42:2,4,15,18 43:2,4 63:12 64:1 70:13 73:23 74:17,24 96:17 98:5</p> <p>understanding 19:2,4,11 21:13 25:9 26:10 35:22 36:3,4 38:22 39:3,11 43:3 44:9 68:23 73:25 84:3</p> <p>understood 36:20 60:19 72:2</p> <p>unfortunate 78:18</p> <p>unique 93:15</p> <p>unit 87:20 90:15</p> <p>units 90:20,23 91:4</p> <p>unpatentable 36:1</p> <p>unpatentable.' 31:20</p> <p>unrelated 43:24</p> <p>unsecured 61:7</p> <p>up-to-date 24:22</p> <p>usage 48:15 49:10,12,17 50:1</p> <p>USB 87:3</p> <p>user 28:10,13,14,23 29:17, 20,21 30:20,23,24 53:1 56:4,5,24 57:3,24 58:20 67:20,22 74:22 83:5 92:3,7,20 93:15,16 94:13,17 95:14 98:15</p> <p>user's</p>	<p>57:10</p> <p>users 28:16 94:15</p> <p>Usman 7:3</p> <hr/> <p style="text-align: center;">V</p> <hr/> <p>valid 21:24</p> <p>valuable 22:13</p> <p>values 79:15</p> <p>vector 59:6</p> <p>verification 50:14,21</p> <p>verifier 55:3</p> <p>verify 55:12</p> <p>version 27:7 32:21,25 33:4,13, 19,21 34:6,7 47:23</p> <p>view 81:2</p> <p>vulnerable 57:15</p> <hr/> <p style="text-align: center;">W</p> <hr/> <p>wanted 6:17</p> <p>Ward 7:1,7</p> <p>ways 89:9</p> <p>weak 57:2</p> <p>weaknesses 15:18 21:22</p> <p>well-known 74:3</p> <p>wholesale 56:16</p>	<p>word 19:23,25 20:6 24:17 77:18</p> <p>work 7:24 18:3 19:19 25:8 39:4,20 40:22 44:7 45:1,3,7 67:9 81:9 88:8</p> <p>worked 24:10 43:14,23</p> <p>working 23:21 24:2 37:2 43:21 59:15 81:14</p> <p>works 15:20 87:25 91:11</p> <p>world 95:11</p> <p>wrap 7:22</p> <p>write 46:18,20 47:7 61:11 80:12 84:21 85:20</p> <p>writing 46:1,3,25 84:11,17,18</p> <p>written 84:15</p> <p>wrong 41:19 85:18</p> <p>wrote 24:7 43:14 46:16,19</p> <hr/> <p style="text-align: center;">Y</p> <hr/> <p>year 27:1 40:8,23 41:1,2</p> <p>years 24:18 26:22 37:5 39:17, 24 40:11 51:20,25</p> <p>young 42:14</p>
--	--	--