

Transcript of the Testimony of:

DR. WENKE LEE

NETSKOPE, INC.

VS.

FORTINET, INC.

December 13, 2023

Volume I



I M A G I N E
R E P O R T I N G

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

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner

IPR2023-00458

Patent 9,280,678 B2

Remote deposition of DR. WENKE LEE
was taken pursuant to notice, beginning at 9:10
a.m. Pacific Time on December 13, 2023, before
Gail Verbano, Registered Diplomate Reporter,
Certified Realtime Reporter, Certified Shorthand
Reporter, and Notary Public, there being present
via videoconferencing:

- - -

1 A P P E A R A N C E S:

2 On behalf of Petitioner:

3 WEI YUAN, ESQ.

4 wyuan@perkinscoie.com

5 BABAK TEHRANCHI, ESQ.

6 btehranchi@perkinscoie.com

7 PERKINS COIE LLP

8 11452 El Camino Real, Suite 300

9 San Diego, California 92130

10 858.720.5700

11

12

13 On behalf of Patent Owner:

14 QUINCY LU, ESQ.

15 quincylu@quinnemanuel.com

16 QUINN EMANUEL URQUHART & SULLIVAN, LLP

17 865 South Figueroa Street, 10th Floor

18 Los Angeles, California 90017

19 213.443.3251

20

21

22

23

24

25

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

- - -
I N D E X
- - -

EXAMINATION OF:	PAGE
DR. WENKE LEE	
By Attorney Lu	5
PREVIOUSLY MARKED EXHIBITS	
	PAGE
Exhibit 1002 Declaration of Wenke Lee in	6
Support of Petition for Inter	
Partes Review of US Patent No.	
9,280,678 B2	
Exhibit 1004 US Patent Application, ...	42
Cidon et al.	
Exhibit 1006 US Patent Application, ...	110
Shifka et al.	
Exhibit 1009 US Patent Application, ...	109
Auradkar et al.	
Exhibit 1011 US Patent Application, ...	174
Chiueh et al.	

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

DEPOSITION SUPPORT INDEX

QUESTIONS INSTRUCTED NOT TO ANSWER:

PAGE LINE

(None)

REQUEST FOR PRODUCTION OF DOCUMENTS

PAGE LINE

(None)

STIPULATIONS

PAGE LINE

(None)

QUESTIONS MARKED

PAGE LINE

(None)

REPORTER'S NOTE:

QUOTATION MARKS ARE USED FOR CLARITY AND DO NOT NECESSARILY
REFLECT A DIRECT QUOTE.

///

///

///

1 December 13, 2023; 9:10 a.m. Pacific Time

2 Remote Deposition of Dr. Wenke Lee

3 - - -

4

5 WHEREUPON,

6 DR. WENKE LEE,

7 being first duly sworn or affirmed to testify to the

8 truth, the whole truth, and nothing but the truth,

9 was examined and testified as follows:

10

11 EXAMINATION

12 BY ATTORNEY LU:

13 Q. Good morning, Dr. Lee.

14 A. Good morning.

15 Q. Can you please state your full name for
16 the record.

17 A. Wenke Lee. W-E-N-K-E, L-E-E.

18 Q. And where are you located today?

19 A. I'm in Atlanta, Georgia.

20 Q. And is anyone else in the room with
21 you?

22 A. No.

23 Q. Do you have any notes or documents in
24 front of you?

25 A. I have printed a clean copy of my

1 declaration, and also a clean copy of the '678,
2 and that's it.

3 Q. So by your declaration, do you mean the
4 declaration you submitted in IPR2023-00458?

5 A. Yes, that's correct.

6 (Exhibit Number 1002 was previously
7 marked for identification.)

8 BY ATTORNEY LU:

9 Q. Okay. Do you have a copy of your
10 declaration that was submitted with the sur-reply
11 in IPR2023-00030?

12 A. So is this for the '678 patent or some
13 other patent?

14 Q. '941 patent.

15 A. Yeah, I have somewhere in my other desk,
16 so ...

17 Q. Well, that's okay, I can --

18 A. Yeah.

19 Q. So let me ask you this first.

20 A. Yeah.

21 Q. Well, first of all, is there any reason
22 why you can't tell the truth today?

23 A. No.

24 Q. Okay. So you understand you were
25 already deposed in IPR2023-00030 against the '941

1 patent.

2 Do you recall that?

3 A. Yes.

4 Q. Okay. And do you understand that today
5 you're here to answer questions about both of
6 these cases, IPR2023-00458 and IPR2023-00030,
7 both the '941 patent and the '678 patent?

8 A. Yes, I do. Yes, I do.

9 Q. Right.

10 A. So you want me to bring my supplementary
11 declaration for '941?

12 Q. No, that's okay. If or when we get to
13 it, I will load it, or maybe you can do it.

14 A. Okay, all right.

15 Q. I'll probably get --

16 ATTORNEY YUAN: Quincy, sorry to
17 interrupt. Can we just do the '678 first, and
18 then we can move on, depend on the timing I guess.
19 We also reserved tomorrow. So after we are near
20 the end of the deposition for '678 IPR, we can
21 move on to '941.

22 ATTORNEY LU: So his '941 supplemental
23 declaration is very short, so my questioning will
24 be pretty limited, if I even do ask any questions.

25 But my plan was, I think the easiest way

1 to do this is just to treat this as one
2 deposition, that we will submit his transcript for
3 both cases rather than passing off the witness and
4 then restarting and things like that. So I think
5 the easiest way is just to treat this as the
6 deposition for both proceedings. But I will begin
7 with the '678 patent.

8 And then at the -- after I'm done with
9 my questioning I'll move on to the '941 patent.
10 But I think the easiest way is just for me to
11 treat this as one proceeding and I don't have to
12 pass the witness back and forth. Is that okay?

13 ATTORNEY YUAN: I would -- I'm going to
14 say that's the way we separate the two
15 proceedings. That would be cleaner record, so
16 that's the way we can separate the questions. I
17 just don't want to, like, somehow cross some
18 questions into another IPR proceeding.

19 ATTORNEY LU: I'm sorry. I didn't -- I
20 didn't catch what you said there.

21 ATTORNEY YUAN: So we would like to have
22 a clean record, just separate for each proceeding
23 instead of having just one.

24 ATTORNEY LU: So you want -- when I'm
25 done with '678, you want me to pass the witness

1 and then we put him under oath again? Is that
2 what you want to do?

3 ATTORNEY YUAN: Yes.

4 ATTORNEY LU: Okay. All right. I guess
5 that's fine. That's not -- we probably should
6 have discussed that beforehand, but that wasn't my
7 understanding. But that's fine.

8 All right. So for the record, I'm only
9 going to be asking questions about 00458. And
10 then when I'm done with that, I'll pass the
11 witness, and then we can restart for the other
12 proceeding.

13 ATTORNEY YUAN: Thanks.

14 BY ATTORNEY LU:

15 Q. Okay. So since -- I don't believe
16 you've been deposed before for IPR2023-00458.
17 Let's just go over some of the basics.

18 You understand you're here to answer
19 questions about your declaration that you
20 submitted with the petition in IPR2023-00458?

21 A. Yes, I do.

22 Q. Did you do anything to prepare for this
23 deposition?

24 ATTORNEY YUAN: I'm going to caution the
25 witness, Dr. Lee, to the extent there's any

1 privileged or work product maybe implicated by
2 your answer, you should not disclose any specific
3 details of your discussion or communication with
4 your attorneys.

5 Go ahead. Go ahead.

6 THE WITNESS: Yes. I prepare, yes.

7 BY ATTORNEY LU:

8 Q. And did you meet with anybody to
9 prepare for this deposition?

10 A. I have discussion with my counsels, yes.

11 Q. And would that be Mr. Yuan?

12 A. Yes, Mr. Yuan and Mr. -- and also Babak.

13 Q. Anybody else, or just those two?

14 A. Just Yuan and Babak.

15 Q. And when did you meet with them?

16 A. A couple times in the last couple weeks.

17 Q. And how long did you meet with them?

18 A. I think total a couple hours. I don't
19 recall the exact number of hours.

20 Q. And did you review any documents?

21 A. Yeah, I reviewed my declaration, of
22 course. The patent owner's preliminary response,
23 and the patents.

24 Q. Okay. Can I turn to your declaration,
25 the '678 declaration.

1 A. Okay.

2 Q. Okay. Well, there's a bunch of
3 exhibits at the end. But could you turn to the
4 last page of the declaration itself, which is
5 page 161.

6 A. Yes. Yes, I'm there.

7 Q. Okay. Is that your signature on that
8 page?

9 A. Yes.

10 Q. Dr. Lee, did you write this
11 declaration?

12 A. Yes, that's my -- yeah, that's my
13 declaration.

14 Q. But my question was, did you, like,
15 write every single word in this declaration?

16 A. No.

17 Q. Did you write any of it?

18 A. Yes.

19 Q. What percentage do you think you might
20 have written for this declaration?

21 A. I have not counted, but I've written and
22 commented and revised throughout the declaration.

23 Q. Did you write the first draft of your
24 declaration?

25 A. I was in the -- in the -- yeah, I was in

1 the same effort writing the draft and also the
2 final version; yes.

3 Q. So you wrote the first draft; is that
4 your testimony?

5 A. I was part of the writing process.

6 Q. When were you first retained by counsel
7 for this matter?

8 A. I don't remember. Maybe more than a
9 year ago. I don't remember the exact date.

10 Q. Dr. Lee, what is a schema?

11 A. Can you give me the proper context of
12 what a schema?

13 Q. Have you ever heard of the term
14 "schema" before?

15 A. Yes, in various context. For example,
16 database schema, that is one way of talking about
17 a schema.

18 Q. Okay. So what is a database schema?

19 A. Database schema essentially encompasses
20 the data model, how the table structures and so
21 on.

22 So again, when you say schema, I have to
23 know your context. Then I give you to the best of
24 my knowledge my understanding of the word
25 "schema."

1 Q. Have you ever heard of a schema for
2 naming things?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: Yeah, so, again, in the --
5 in naming -- so basically it's explaining how you
6 name things. I mean, that's what schema normally
7 means in this context, similar to the database
8 schema, like, how data is being organized. So I
9 would say the naming schema essentially meaning
10 how names are being created and how names are
11 being managed.

12 BY ATTORNEY LU:

13 Q. So when you say how names are being
14 created, do you mean like it defines how -- like
15 the scope of the possible names you can name,
16 whatever it is you're naming?

17 ATTORNEY YUAN: Objection; form.

18 THE WITNESS: So, again, it really
19 depends on the application context. So can be
20 some naming convention. Can be, you know,
21 formatting -- format the names and so on and so
22 forth. Can be many things.

23 So essentially trying to explain, like I
24 said, similar database, schema context, naming
25 schema just talks about names, how name is being

1 used, how name is being formed.

2 Again, the precise scope of the
3 definition schema really, we have to look at the
4 precise context and scope of the application.

5 BY ATTORNEY LU:

6 Q. So you keep saying it's similar to a
7 database schema.

8 A. Hold on. What I meant is that similar
9 to the -- to the -- how I explained database
10 schema is really, we have to know first the
11 context, right? So database, which is naming, and
12 so the schema really explain how things are being
13 organized, the model and so on and so forth.

14 But again, you know, if you asked me
15 most specific exactly what I mean, I need to look
16 at the context verification -- you know, say
17 naming, exactly what naming, what kind of naming
18 you're talking about, right?

19 Q. So why don't we begin in the context of
20 databases.

21 What -- what exactly are you defining in
22 a database schema?

23 A. So database schema will start with --
24 for example, are you using relational database,
25 graph database and so on and so forth, right? And

1 then you say, Hey, you've organized a relational
2 database, you know, what kind of -- what kind of
3 organization you want to put in to -- when you
4 organize the table, and how do -- do you support
5 certain sort of basic operations, you know, like
6 linking and -- and -- you know, views and so on
7 and so forth.

8 So, I mean, like I said, "schema" is
9 very high-level term. So if you want to keep
10 asking specific things, I will actually need to
11 know exactly what application referring to.

12 Q. Right. I'm asking in the context of
13 databases at the moment.

14 So does the schema define, like, what
15 sort of data you can put into the database?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: Normally, I mean, database
18 supposed you able to store anything you want in
19 data. So, I mean, I wouldn't say this data --
20 database schema only tells you can only store
21 text. I haven't seen that like.

22 Again, some application may say, Hey, I
23 only want to store text and they have -- they may
24 have a customized specific schema for that. But
25 normally when we talk about database schema, we

1 normally don't say, Hey, this only for particular
2 type of data.

3 But like I said, Normally, we tell
4 people -- give some people ideas, say, how data is
5 being organized. Like I said, is it relational
6 versus graphical versus object-oriented you, name
7 it. I mean this -- yeah.

8 BY ATTORNEY LU:

9 Q. I'm not a technical expert, but -- so
10 would a database schema include something like
11 the name of a table and the names of the columns
12 for that table, for example?

13 A. I would say those are things you expect.
14 That schema will -- would include but doesn't have
15 to include. Like I said, when you apply this
16 concept of having a schema to application, you
17 look at a specific application and say, ah, for
18 this application maybe -- maybe, you know, I don't
19 need to -- for example, all I need is organize the
20 files as -- as a table. I mean, you know,
21 whatever.

22 So, I mean, so, again, like I said,
23 normally database schema would tell you the model
24 of data, meaning how data is being stored, what's
25 the relationship among the data that you store and

1 so on. Those are normally things at least
2 personally that's what I look for.

3 And, yeah, sure there's -- normally when
4 we look at these things in detail, you expect the
5 table has a name, the column -- the columns would
6 have names. But -- but, again, the schema would
7 not tell you exactly -- would not require the
8 names have to be certain types or certain format.
9 Those are details really up to the implementation
10 and also the applications.

11 Q. Are you familiar with the term "URL"?

12 A. Yeah.

13 Q. And what does that stand for?

14 A. If I recall correctly, I think it stands
15 for universal resource locator.

16 Q. Okay. And, for example,
17 HTTP://Google.com, is that an example of a URL?

18 ATTORNEY YUAN: Objection; form.

19 THE WITNESS: So, again -- I would say
20 www.Google.com, sure that's a URL.

21 BY ATTORNEY LU:

22 Q. And is the format of a legal URL
23 regulated by a schema?

24 ATTORNEY YUAN: Objection; form.

25 THE WITNESS: I wouldn't go that far and

1 say legal is not legal. It's basically whether
2 the URL is --

3 BY ATTORNEY LU:

4 Q. Valid, I should say.

5 A. Valid.

6 Q. Is it regulated by a schema?

7 ATTORNEY YUAN: Objection; form.

8 THE WITNESS: So, again, I don't know
9 whether they use the term "schema" or not. I'm
10 sure if you look at some of the documents or
11 standards, they would tell you what to expect when
12 you start to use a URL. If you want to -- want
13 the URL to be valid, what elements -- you know,
14 what are the required elements, what are optional
15 elements and so on and so forth.

16 Whether they use the term "schema" or
17 not. I don't know. Could be. I've seen places
18 where they use the term "schema."

19 So -- but, again, without referring to
20 you know, the www standard documents, I cannot
21 tell you whether they use the term "schema" or
22 not.

23 BY ATTORNEY LU:

24 Q. Well, putting that aside, the
25 terminology, for a URL, for example, you can't

1 just enter any string of text and that would be a
2 valid URL; right? It would have to be formed in
3 a particular manner; is that correct?

4 ATTORNEY YUAN: Objection; form.

5 THE WITNESS: So, again, depends on the
6 context, right? If you entered that in let's say
7 a Google search bar, it would suggest, Do you mean
8 this URL? It should suggest you to guess what
9 you're trying to do.

10 So is that valid? It depends. I mean
11 your grandmom say that's perfectly valid. Your
12 grandma doesn't want to write www or .com at the
13 end. So it really depends, right?

14 BY ATTORNEY LU:

15 Q. But wouldn't a valid URL require, for
16 example, the protocol that you're using, such as
17 HTTP or FTP?

18 ATTORNEY YUAN: Objection; form.

19 THE WITNESS: So, again, depends on
20 where you use, right? So let's say you put this
21 URL on the address bar of, let's say, a browser
22 and the browser would just expect, just by
23 default, try to put HTTP or HTTPS and assume, by
24 default, it's an HTTP protocol, unless they
25 specifically say, file, colon, slash, slash,

1 whatever, your local drive, the browser knows,
2 okay, you want to browse your home directory --
3 file directory in your machine.

4 So meaning that by default, you know, I
5 think a browser would assume it's HTTP. And some
6 people like me would actually type out the whole
7 thing just to be sure, right? So ...

8 BY ATTORNEY LU:

9 Q. So but a URL at least can include the
10 protocol like HTTP; is that right?

11 ATTORNEY YUAN: Objection; form.

12 THE WITNESS: Like I said, some of these
13 things are -- how I put it? You know, like I
14 said, without reading the standard documents, I
15 mean, I really don't know what they suggest people
16 should provide, should not or don't have to
17 provide.

18 But on the other hand, the flip side is
19 that, you know, companies like Google and all
20 these vendors, when they ship a browser to you,
21 they try to really help the user, right? They try
22 to guess what the user is wanting to do and then
23 either suggest or by default go to that -- you
24 know, go to a particular site, meaning essentially
25 that somebody's browser would fill out some of

1 these quote/unquote missing or optional terms for
2 you.

3 BY ATTORNEY LU:

4 Q. But so you said there, "without reading
5 the standard documents."

6 So is it your testimony that there are
7 standards with respect to how -- what constitutes
8 a valid URL?

9 ATTORNEY YUAN: Objection; form.

10 BY ATTORNEY LU:

11 Q. Let me withdraw that question.

12 Is it your testimony that there is some
13 sort of document that is a standardized document
14 that defines what a valid URL is?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: So let me put it this way.
17 I haven't read the document since the article
18 1990s, so I don't know for sure. But I'll be
19 surprised if they don't talk about what's a URL
20 and -- but whether they then say, Hey, that's
21 required, what's not required, that -- those
22 details I don't know.

23 I'm sure they define what URL is and
24 give plenty of examples. I am very sure about
25 that. I'll be shocked if it's not.

1 Again, like I said, I'm going to qualify
2 and say I haven't checked out document for a long
3 time --

4 BY ATTORNEY LU:

5 Q. Sure.

6 A. -- and this www standard organization,
7 that actually has all kind of these documents,
8 yeah.

9 Q. Understood. And that's okay. I mean,
10 I also haven't looked at that in a very long
11 time.

12 Can you turn to your declaration --

13 And sorry. For the court reporter,
14 this is Exhibit 1002 in IPR2023-00458.

15 Can you turn to paragraph -- let me
16 see, what's a good paragraph.

17 Paragraph 42. It's on page 14. And
18 also 41, if you want to review both of those
19 paragraphs.

20 (Witness reviews document.)

21 A. Okay.

22 Q. So in paragraph 41, the latter half of
23 that paragraph you say:

24 "Mika et al. tabulated the most
25 commonly used namespaces for URLs in its

1 Table 5 (see below), illustrating that a
2 namespace for URLs can have different
3 sections, such as a domain name (e.g.
4 www.facebook.com) and a subdirectory,
5 (e.g., 2008)."

6 And then you cite to Exhibit 1021, and
7 on the next page you can see Table 5.

8 Do you see that?

9 A. Yes, I see that.

10 Q. What is a namespace for URLs?

11 A. So at the beginning of paragraph 42,
12 right, I basically explain that a namespace
13 ensures that every object within the context of
14 the namespace that we're talking about -- you
15 know, if it's in the -- it's in the context of the
16 namespace, an object can be uniquely identified by
17 the name. So the namespace for the URL
18 essentially is what we're looking at the Table 5,
19 which means that everything -- every sources --
20 every source in the context of this table is
21 uniquely identified by the URL.

22 Now, of course, we talk about can be,
23 you know, hierarchy as well, which means that
24 maybe under, let's say, Facebook you have multiple
25 subdirectory, there's 2007/2008, so on and so

1 forth. But within the context of, let's say,
2 Facebook.com, 2008 is uniquely identified by
3 /2008. 2007 would be uniquely identified by
4 /2007. That's what a namespace is about.

5 Q. All right. So let's look at Table 5.

6 So the first row in Table 5 says that
7 there's a name space called ogp.me/ns#. And then
8 it says, at least in 2001, there are 493 million
9 URLs using this namespace; is that right?

10 A. That's what the table says. I haven't
11 done my own research on that one.

12 Q. So this table isn't saying there were
13 493 million URLs that had the domain name
14 ogp.me/ns#; right?

15 A. So the way I understand this table is
16 that it refers to -- so on the left-hand side
17 the -- we talk about the URLs. And each URL, you
18 can think of it as a -- each URL essentially is a
19 namespace in -- in this case. It's almost like,
20 here is let's say Facebook 2008. So that's a
21 namespace of what?

22 Namespace of everything under that 2008.
23 Could be a ton of things within that. It's almost
24 like what -- I tell you, hey, let's say imagine on
25 the left-hand side I list all the high-level file

1 directories in, I don't know, let's say,
2 Amazon.com, whatever the cloud server. Then
3 each -- each directory I list here is a namespace.

4 And then on the right-hand side column,
5 when you talk about the URLs, that means number of
6 unique URLs within that namespace. For example,
7 let's say, Facebook.com/2008, has, I don't know,
8 150 million URLs within that subdirectory, can be
9 something-something Wei, something-something
10 Baback, something-something Wenke. Who knows,
11 yeah.

12 That's what it is. Meaning that these
13 actually -- I mean, of course you can say, hey,
14 then what about all these top-level things that we
15 list on the left-hand side collectively?
16 Collectively, you can call it, that belong to
17 another namespace. Can we say a namespace of
18 bunch of high-level URLs being studied. That's
19 how I read it.

20 Q. All right. So your understanding is
21 that -- sorry. I had the date wrong before.

22 So your understanding is that in 2008
23 there are 26 million URLs under
24 www.w3.org/1999/02/22-rdf-syntax- ns#? That's
25 your testimony?

1 ATTORNEY YUAN: Objection to form.

2 THE WITNESS: So what I'm trying to say
3 is that this namespace means that, on the
4 right-hand side column, it talks about the
5 namespace. And so this name says identified by
6 www.Facebook.com/2008.

7 On the right-hand side is the meaning of
8 URLs, meaning that within the namespace, what are
9 the unique objects? And those are unique objects.
10 Each unique object is identified by URL. So the
11 universal source locator pointing to the object.
12 What's the object there? It can be a -- can be
13 a -- can be a page, can be, you know, a image
14 file, whatever.

15 BY ATTORNEY LU:

16 Q. So maybe this will help clarify. Could
17 you pull up a browser window.

18 A. Okay.

19 Q. And then can you enter that third row,
20 www.w3.org/1999/02/22-rdf-syntax-ns#.

21 A. Hold on.

22 Q. And if you're not able to do that --

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Yeah, sure, I can try
25 that.

1 BY ATTORNEY LU:

2 Q. And I can just upload a printout of
3 what you get when you go to that URL.

4 ATTORNEY YUAN: Objection; form.

5 THE WITNESS: It says "document not
6 found."

7 BY ATTORNEY LU:

8 Q. Well, you probably entered it wrong,
9 because I'm able to enter it -- or maybe -- I
10 don't know.

11 A. Hold on. Hold on.

12 ATTORNEY YUAN: Objection; form.

13 THE WITNESS: I didn't exactly -- not
14 what you told me, www. HTTPS probably is not --
15 let me try FireFox because FireFox is probably
16 more forgiving.

17 It seems that file not found.

18 BY ATTORNEY LU:

19 Q. Okay. Well, let's just put that aside.
20 So I uploaded to the chat a document.
21 It's not an exhibit in this case, but why don't
22 you download that and take a look.

23 ATTORNEY YUAN: Objection; form.

24 ATTORNEY LU: Counsel, what's the basis
25 of your objection?

1 ATTORNEY YUAN: So this exhibit is not
2 in the record.

3 ATTORNEY LU: Okay. It is in the record
4 now because we're part of this deposition. I'm
5 not limited to just the exhibits that were
6 submitted.

7 Also, I'm hearing an echo.

8 But as far as, you know, relevancy, this
9 is obviously --

10 ATTORNEY YUAN: Foundation. Also
11 objection; foundation.

12 ATTORNEY LU: Okay. Understood.

13 BY ATTORNEY LU:

14 Q. Dr. Lee, did you download --

15 A. Yep. Yep.

16 Q. I will submit that this is the document
17 that you get when you enter that third namespace
18 into a browser window.

19 A. Okay. I will just say that I tried and
20 say "file not found." That's what I got.

21 Q. Okay. You probably did it wrong, but
22 that's okay.

23 I'm hearing an echo again.

24 So, Dr. Lee, does this -- are you
25 familiar with this sort of document before? Have

1 you seen this sort of document before?

2 ATTORNEY YUAN: Objection; form.

3 THE WITNESS: I don't remember last time
4 I saw it. No, I'm not familiar with that, no.

5 BY ATTORNEY LU:

6 Q. Okay. Do you see near the top of the
7 page there's something called a dc:description?

8 ATTORNEY YUAN: Objection; form.

9 THE WITNESS: Which line you're looking
10 at? Okay, DC, okay.

11 BY ATTORNEY LU:

12 Q. The eighth line.

13 A. Is the prefix DC?

14 Q. No, "dc:description," it's the eighth
15 line.

16 A. So is it the top of the first page
17 you're talking about? Are you still talking about
18 the PDF that you uploaded?

19 Q. Yes, I am.

20 A. Looking at the first page? Which page?

21 Q. I'm looking at the first page.

22 A. Okay. Which line?

23 Q. Roughly the eighth line.

24 A. Eighth line.

25 ATTORNEY YUAN: Objection; form.

1 ATTORNEY LU: Counsel, there's no
2 question.

3 THE WITNESS: Yeah, yeah,
4 dc:description. I see it, yeah.

5 BY ATTORNEY LU:

6 Q. And the description says: "This is the
7 RDF Schema for the RDF vocabulary terms in the
8 RDF Namespace, defined in RDF 1.1 Concepts."

9 Do you see that?

10 ATTORNEY YUAN: Objection; form.

11 THE WITNESS: I see that, yeah.

12 BY ATTORNEY LU:

13 Q. Can you tell me what this means?

14 ATTORNEY YUAN: Objection; form.

15 THE WITNESS: It means what it says:
16 Basically, explain the vocabulary, I guess.

17 BY ATTORNEY LU:

18 Q. What does that mean, to explain the
19 vocabulary?

20 A. I think -- I think, I mean, for example,
21 they explain what HTML is, what the language
22 string is, literal means. I think it -- yeah.
23 Maybe those are examples.

24 Again, I'm not -- I haven't spent enough
25 time studying this document to say. I'm just

1 guessing based on, you know, common knowledge of
2 what a schema could be.

3 Q. And so it's your opinion that this at
4 least resembles a schema?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: Like I said, schema can be
7 very broadly defined. I mean, if that -- if they
8 say that's -- that's the definition schema, I
9 mean, yeah, I can take that schema defining some
10 of the vocabulary, yeah. I mean, that's -- I will
11 agree that's part of a schema's job, meaning
12 that's all schema does? No, schema can do many
13 other things too, so ...

14 BY ATTORNEY LU:

15 Q. Okay. We can put that away.

16 Going back to your declaration at
17 paragraph 42, you say, "In fact, namespaces can
18 have a flat structure forming a single collection
19 of unique names."

20 And then, "As explained in Balakrishnan,
21 et al. (2004), a namespace in a flat structure can
22 simply be a number chosen from within a range
23 e.g., 0 to 2 to the 128 minus 1."

24 Did I read that right?

25 A. Yes.

1 Q. So at least in Balakrishnan, the
2 namespace there is that it defines names that can
3 be some sort of number between 0 to 2 to the 128
4 minus 1; is that right?

5 A. Yeah, that looks like what it says, yes.

6 Q. Okay. So the string ABCD, that would
7 not be within this namespace defined by
8 Balakrishnan; is that correct?

9 ATTORNEY YUAN: Objection; form.

10 THE WITNESS: Doesn't have to be
11 excluded. I mean, you know, but the point is that
12 you want to have some way of naming -- naming
13 things within this range. You could add this
14 number to a string. I mean, there's many things
15 you can do, yeah.

16 BY ATTORNEY LU:

17 Q. Of course there's many things you can
18 do. But at least here, in the way you've written
19 it, you say, "A namespace is a flat structure.
20 Can simply be a number chosen from within a
21 range."

22 And, you know, the string ABCD is not
23 within a range 0 to 2 to the 128 minus 1; is that
24 right?

25 A. So what I said here is "can simply be."

1 Doesn't say has to be. See what I'm saying? So
2 that it's not exclusive. I didn't say exclusively
3 you can only use number. Meaning immediately
4 suggest, yeah, it can be as simple as a number.

5 Q. So your namespace can be as simple as a
6 number; is that right?

7 A. If you want to, yeah, sure. Why not?

8 Q. So I do want to. Let's say I do want
9 to have a namespace that is defined as a number
10 within a range from 0 to 2 to the 128 minus 1.

11 Are you with me?

12 A. Yes.

13 Q. The string ABCD would not fall within
14 that namespace that I've defined; right?

15 A. If you define --

16 ATTORNEY YUAN: Objection to form.

17 THE WITNESS: Again, if you define your
18 names to be -- can only be numbers then, of
19 course, the string ABCD would not be allowed by
20 your -- by your schema or whatever you want to
21 call it, yeah.

22 BY ATTORNEY LU:

23 Q. Okay. And then also, moving on:

24 "As another example, a namespace
25 can provide the scope or the context of

1 identifiers, e.g., variables, functions,
2 et cetera, in a program such that an
3 identifier is referred to by its unique
4 short, local name within the namespace
5 and by its unique fully qualified name
6 (e.g., that includes the name of the
7 scope) from outside the namespace."

8 Could you explain what you mean in that
9 sentence.

10 A. So what I mean here is that really the
11 namespace does have a scope of the objects that
12 it's identifying. Meaning that the namespace's
13 own scope -- for example, if this namespace is for
14 files within that directory, then each file within
15 that directory can have a very short name. Can be
16 just -- let's say very short string.

17 But then each file within that
18 subdirectory can also be identified by a full,
19 qualified name, a long name, meaning that includes
20 the name of the directory, which -- and the parent
21 directory, which is outside the scope of the
22 directory and so on and so forth. So, for
23 example, you can say /home/Wenke/documents.

24 I would say, let's say document is the
25 namespace. Every file within the -- within the

1 document subdirectory can have a short name. But
2 each file in the directory of documents also has a
3 unique fully qualified, long name, which is
4 /home/Wenke/documents/filename. So that's what I
5 said.

6 Q. Okay. Let me try to break this down a
7 little bit.

8 So you refer to a unique short local
9 name within the namespace; right?

10 A. Within -- let's say in the example
11 that's you gave, which just be, if the current
12 namespace is the document directory, then each
13 file within the document directory can have a
14 unique name within the document directory.

15 Now, let's say if I name a file called
16 "Foo," the same file Foo can also exist in
17 /home/Wei, okay? But within /Wenke is unique.
18 It's called Foo.

19 Another file also called Foo -- F-0-0
20 for the record -- is also unique within Wei's
21 subdirectory, okay?

22 And said, well, will I be confused? No,
23 because within each namespace, we're talking about
24 within this namespace, this file Foo is unique,
25 okay? Then the name is unique within this

1 directory.

2 Now -- yeah. And then the fully
3 qualified name, meaning the
4 /home/Wenke/documents/Foo, of course, will be
5 different from /home/Wei/documents/Foo, because
6 fully qualified all the way from, you know, the
7 root directory. That's what we're talking about
8 here.

9 Q. Okay. Maybe we should start with the
10 unique fully qualified name.

11 So in your example, you said /home
12 slash --

13 A. -- Wenke/documents/Foo.

14 Q. Okay. Wenke/documents/Foo.

15 A. And for the record "slash" means that
16 you -- actually the root of your -- of your hard
17 drive. There's no other place to go. Just to be
18 sure. That's the end of the universe -- or
19 beginning of the universe, whatever you want to
20 call it.

21 Q. Okay. Understood.

22 So you refer to the name of the scope.
23 So in your example, would the name of the scope
24 be /home/Wenke/documents?

25 A. That's not what I'm talking about. I'm

1 talking about -- when you talk about namespace,
2 first of all you talk about what's a scope of this
3 current namespace. The namespace is documents.
4 That means the scope is everything within the
5 directory documents.

6 Q. Okay. So maybe -- maybe you
7 misunderstood my question.

8 So in paragraph 42 you say -- you refer
9 to a "unique fully qualified name (e.g., that
10 includes the name of the scope)."

11 And so within your example of a unique
12 fully qualified name -- i.e.
13 /home/Wenke/documents/Foo -- which part of that
14 name is the name of the scope?

15 A. The name of the scope is "documents."
16 Okay, and also I said by -- it's "unique fully
17 qualified name (e.g., includes the name of the
18 scope) from outside of the namespace."

19 So basically I also talk about
20 /home/Wenke. So those are outside of the
21 documents namespace.

22 So, again, when I say "documents," the
23 namespace is within documents. So that's why I
24 say you want to include -- the name of the scope,
25 you can say, hey, the name of the scope, you say

1 what's the scope of these names? Well, it's
2 documents.

3 But you say what's the fully qualified
4 name -- a fully qualified scope of these files?
5 The fully qualified, you would include names,
6 other than -- how to put it? -- you would include
7 the parent directory of documents, which is
8 /home/Wenke.

9 Q. Okay. And then within your example,
10 the unique short local name would be Foo; right?

11 A. Within the -- within the namespace of
12 documents, yes. Yeah.

13 Q. One of the unique short local names
14 within the namespace of documents would be Foo in
15 your example?

16 A. As I say, in paragraph 42, I basically
17 say that, you know -- a namespace provide the
18 scope the context of identifier. So -- so let's
19 say -- let's say files, or the name Foo.

20 So in this case, you know, the name is
21 unique within its namespace. Again, examples the
22 namespace is -- is the subdirectory document. So
23 Foo is a unique name within the subdirectory.

24 Q. That's why you say "unique short local
25 name"; right? It's unique within -- the local

1 name is unique; is that right?

2 A. Yeah, local name within the space --
3 meaning that the -- every identifier is -- when
4 you talk about namespace, talk about essentially a
5 scope of what are these objects.

6 And then -- and then the purpose of
7 namespace, as I said at the beginning of 42, is
8 that every object within the context of the
9 namespace can be unique -- identified uniquely by
10 its name.

11 So that's exactly what the example here
12 I try to provide is that, you know, let's say the
13 document -- we say, hey, the document is
14 namespace. Then we just basically know that every
15 file within this document namespace, which is the
16 directory, every file within this directory would
17 be uniquely identified by its name within this
18 directory.

19 Q. And so you refer to a document's
20 namespace.

21 There could be other namespaces within
22 your file system; right? You could have like a
23 music namespace with files within that directory;
24 is that right?

25 ATTORNEY YUAN: Objection.

1 THE WITNESS: That's correct.

2 BY ATTORNEY LU:

3 Q. And maybe those files would be, like,
4 music files that have also their own unique short
5 local name; is that right?

6 A. I'm sorry. Can you repeat the question
7 again?

8 Q. And so -- let me repeat it.

9 So in the music namespace, you may have
10 music files that are identified by their unique
11 short local name; is that right?

12 ATTORNEY YUAN: Objection; form.

13 THE WITNESS: So, again, you have to be
14 careful, meaning that unique within its namespace,
15 then so -- so depends on how you organize your
16 music, right? Can be -- you can say within the
17 namespace of each album then -- assuming that each
18 piece within the album is uniquely identified by
19 the name within that scope, within that namespace,
20 right? Yeah.

21 BY ATTORNEY LU:

22 Q. Of course an object doesn't have to be
23 identified by its file name; right?

24 I know that's typical in a file system.
25 But you could have a file system that doesn't

1 treat the file name as the unique short local
2 name; is that correct?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: I don't know how you can
5 organize your data -- I mean, the point is that
6 every file within the directory should be uniquely
7 identified. That's all. It's simple, yeah.

8 BY ATTORNEY LU:

9 Q. Have you ever heard of the term "file
10 ancestry"?

11 ATTORNEY YUAN: Objection; form.

12 THE WITNESS: Yes.

13 BY ATTORNEY LU:

14 Q. So suppose I have a file and I copy and
15 modify it in some way. The original file that I
16 have is the parent file, and the modified file is
17 a child file.

18 Is that your understanding?

19 ATTORNEY YUAN: Objection; form.

20 THE WITNESS: I mean, I rather you point
21 me to -- I remember reading it from one of the
22 patents -- could be '678 -- that talks about
23 ancestry. Either that or Cidon.

24 But, you know, I mean, if you want to
25 ask this question in the context of this case, I

1 would rather you point me to the -- to the patent
2 language so that I -- I can qualify my answer more
3 precisely within the context of the -- of this
4 case.

5 BY ATTORNEY LU:

6 Q. Okay. Sure, if that would help. I am
7 referring to Cidon.

8 A. Okay. Which I don't have it printed
9 out.

10 Q. You don't have it? Okay, let me upload
11 it then.

12 Okay, so when it's done uploading, this
13 is going to be Exhibit 1004.

14 A. Okay.

15 (Exhibit Number 1004 was previously
16 marked for identification.)

17 BY ATTORNEY LU:

18 Q. So if you go to paragraph -- that's not
19 the right one. Let's see.

20 Why don't we go to paragraph 135, and
21 this is on page 8.

22 A. Okay, yeah.

23 Q. And so there's some -- let me know when
24 you're there.

25 A. I'm here, yeah.

1 Q. So it provides some metadata field
2 examples. And then if you go to paragraph 142,
3 one of the examples, is, quote: "File ancestry
4 information such as: Copied from, moved from,
5 created from, version of."

6 Do you see that?

7 A. Okay, yep.

8 Q. Does this mean that the ancestry
9 information for a file includes which file it was
10 copied from?

11 A. Yes.

12 Q. Okay. So if I have a file and I copy
13 it, the copy would be a child of the original
14 parent file; is that correct?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: I don't know exactly the
17 term they use, child or not. But like -- like
18 what paragraph 142 says, basically it tells you,
19 hey, the ancestry information is such that this
20 file is copied from which file. Yeah.

21 BY ATTORNEY LU:

22 Q. So why don't we turn to, like,
23 paragraph 191 which is on page 10.

24 A. Okay.

25 Q. And why don't you read to yourself

1 paragraph 191 through 195.

2 A. Okay.

3 So starting paragraph 191: "In
4 addition to file similarities" --

5 Q. You can read it to yourself.

6 A. Okay.

7 Q. If you want to read it, go ahead.

8 A. That's fine. That's fine. Okay. I
9 misunderstood your question.

10 (Witness reviews document.)

11 A. Yeah, yeah, finished reading, yeah.
12 Yeah.

13 Q. All right. So this passage is talking
14 about some sort of file ancestry tree; is that
15 right?

16 A. Let me see the term here.

17 Yeah, ancestry tree, yes.

18 Q. And so you have a tree structure where,
19 let's say, at the very top the root node you have
20 a file, and then underneath it a parent file, and
21 then underneath it you have some leaf nodes that
22 are child files, for example, right?

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Let me see.

25 Yeah. So it generally define kind of

1 child relationship, let's say B -- how do we
2 determine whether B is a child of A? You know,
3 what 191, 192, 193, 194 talks about, you know,
4 three possible conditions that would make you
5 determine that B is a child of A.

6 BY ATTORNEY LU:

7 Q. And then in 195 it says, "Since a
8 parent file A may have multiple children, this
9 creates a tree structure rooted at the first
10 version of a file, termed the 'ancestry tree'. "

11 Do you see that?

12 A. Yes.

13 Q. What does it mean by first version of a
14 file being the root of the tree?

15 A. It -- I mean, at least the paragraph
16 here they did not discuss what's first version.
17 So I would guess that, you know, looking at 193,
18 can be something that's dated the earliest.

19 Q. So if I have a file and then I copy it,
20 the original file would be the parent file and
21 then the copy would be the child file; is that
22 right?

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Yeah, I mean, really -- it
25 really, like I said, you know, what is -- didn't

1 say here -- so let's say you copy -- let's say B
2 is direct copy of A. But if B is not anywhere in
3 this repository or something, then that -- that
4 connection is lost. Meaning that you have to
5 copy, you know -- let's say B is copied from A,
6 and then B hangs around, and you assume that when
7 you copy the day -- the B stays a little bit --
8 the B is later than A and so on. All this
9 information is there, then, yeah, according to
10 193, then B is a child of A.

11 BY ATTORNEY LU:

12 Q. Okay. You said -- you were talking
13 about being in a different repository. So
14 paragraph 195 does say: "Note that such files in
15 a single ancestry tree may belong to different
16 repositories and different users and is not
17 related to the folder tree structure."

18 A. I understand what you're saying. If you
19 read my deposition more carefully, I will just
20 said that if B is around in this world, so -- you
21 know, whether in this directory or some other
22 directory, it is around, that can be considered --
23 can be considered whether it's a child of A.

24 But it's -- I don't know, if somehow
25 magically disappear or goes to some other place,

1 there's no reason should be this organization or
2 in any of the repositories that this organization
3 would use, basically it's -- it may disappear out
4 of the scope, then you cannot -- because, you know
5 how to put it. Maybe I'm being, I don't know, too
6 academic here. Meaning that, when I say the only
7 way you can determine that B is a child of A is
8 that B is still around, same repository or not
9 doesn't matter. Meaning that you can find it and
10 then you can find the date and say, okay, yeah,
11 it's a copy from A, it's dated after A, so that's
12 why it's a child of A.

13 But if B is not around for whatever
14 reason, then you cannot say that. So you don't
15 even know that B -- you may not even know B
16 exists.

17 So maybe that's completely -- how to put
18 it -- not relevant to this case. But anyway,
19 yeah.

20 Q. I understand what you're saying.

21 So it does say that such files in a
22 single ancestry tree may belong to different users
23 as well.

24 So if A -- my original A file and then I
25 make a copy and call that B and I send that to

1 you, B is still a child of A; right? According
2 to --

3 ATTORNEY YUAN: Objection to form.

4 THE WITNESS: So, again, we have to go
5 through the -- the -- the patent paragraph 192,
6 193 and 194, meaning that -- one of these
7 conditions are met, then, yes -- yeah, I think all
8 the conditions have to be met.

9 Meaning they're similar -- A and B are
10 similar, B is dated after A, and then there's no
11 other things between B and A in terms of
12 similarity. If all three conditions are met, and
13 also B and A are still around for you to consider
14 all these conditions then, yeah, B is a child of A
15 regardless who owns B or who owns A, because 192,
16 193, 194, did not say anything about that -- did
17 not require they belong to the same user or did
18 not require -- as 195 said, they do not require
19 that they are in the same repository.

20 BY ATTORNEY LU:

21 Q. Okay. And actually so 192 says A and B
22 are similar.

23 They don't have to be identical; right?

24 A. So, again, I think that's really
25 subject to the application, how to define

1 similarity, right? Seems to me that's an
2 application specific thing that they can decide,
3 right. You mean, what does -- let's say 194.
4 What does $\text{sim}(S_a S_b)$ mean? Basically the
5 similarity, how to calculate the similarity.
6 Again, application-specific.

7 Q. I assume "sim" in 194, that means the
8 similarity.

9 A. Measure, yes. But, again, they did not
10 say exactly how they're measuring it, and they
11 also did not say exactly how they determine A and
12 B are similar enough. So, again, those things are
13 application-specific stuff.

14 Q. Yes, of course.

15 But at least the fact that you do have a
16 similarity measure means that A and B don't have
17 to be identical; right?

18 A. Seem to be suggesting that, yeah. I'll
19 agree.

20 Q. Okay. Now, if you go to -- on the same
21 page of this patent, if you go on the right-hand
22 column --

23 A. Okay.

24 Q. -- starting at paragraphs 206 --

25 A. Okay.

1 Q. -- through 213.

2 A. Okay.

3 Q. Even like 217 -- why don't you read
4 that to yourself.

5 A. You say start with 206?

6 Q. Yeah, and then all the way to 217.

7 A. Okay.

8 (Witness reviews document.)

9 A. Okay.

10 Q. All right. So this portion is talking
11 about something called a placement policy; is
12 that right?

13 ATTORNEY YUAN: Objection; form.

14 THE WITNESS: I mean, that's what 206
15 says. You know, they essentially suggest -- well,
16 I mean, talks about placement policies based on
17 similarities and ancestry trees.

18 BY ATTORNEY LU:

19 Q. Right. And so 207 it says:

20 "Policies can be defined on
21 documents which are ancestors of other
22 documents. For example, inheritance
23 rules can be defined which imply that a
24 policy that is defined on a document
25 that is rooted at an ancestry subtree by

1 its file metadata or its folder metadata
2 can be extended to its subtree."

3 Did I read that right?

4 A. Uh-huh.

5 Q. So is that saying that you could have a
6 placement policy for a file and then that
7 placement policy would have to apply to all of
8 its child files? Is that what it's saying?

9 A. Basically it's saying that, you know.

10 Yeah, I think that's what -- try to
11 explain inheritance rules, in that the policy
12 that's defined on the document that's rooted in
13 the ancestry subtree by its file metadata or its
14 photo metadata can be extended to its subtree,
15 yeah.

16 So they essentially inheriting, meaning
17 that files in the subtree is inheriting
18 the -- you know, the policies for that -- for
19 the -- for the root of the subtree, yeah
20 basically.

21 Q. And so, for example, the placement
22 policy, as it says in 209, can include placement
23 in specific directories or shares; right?

24 ATTORNEY YUAN: Objection; form.

25 THE WITNESS: Yeah, so basically, you

1 know, paragraph 209, 210, 211, 212 just give you
2 examples of the policies. So like placement,
3 access and sharing permissions, copy control
4 encryption. Those are examples.

5 BY ATTORNEY LU:

6 Q. So for the placement example -- so for
7 example, let's say I have a placement policy for
8 a file that says this can only be placed in
9 /home/Wenke/documents.

10 Is that something that this reference is
11 contemplating?

12 ATTORNEY YUAN: Objection; form.

13 THE WITNESS: So, again, those are
14 specific things, right? Whether they say the
15 placement is such that you have to be in the same
16 directory or nearby directory or directory name by
17 similar names or don't place in the same place --
18 I don't know. I mean, it's really depending on
19 security of -- I mean, security can be also
20 efficiency. There are many other considerations.

21 BY ATTORNEY LU:

22 Q. Uh-huh. So in my example, I have a
23 file, right, and I apply a placement policy on
24 that file.

25 A. Uh-huh.

1 Q. It says this file is restricted to the
2 home/Wenke/documents directory.

3 Are you with me?

4 A. Yes.

5 Q. Okay. So if I make a copy of that
6 file, that copy could inherit the placement
7 policy that I placed on the original file; is
8 that right?

9 ATTORNEY YUAN: Objection; form.

10 BY ATTORNEY LU:

11 Q. At least that's what Cidon says; is
12 that correct?

13 A. I mean, I think they're the stretching.
14 I don't read that from the patent, right?

15 It talks about, yes, you can inherit
16 placement policy, then give you some examples of
17 policies, including 109 talks about placement in
18 specific directories or trees, but did not say --
19 did not imply one way or the other that just
20 because the two files are similar or the
21 parent/child relationship they have to be the same
22 directory or nearby directory or different
23 directory. They didn't say anything like that.
24 So I do not want to draw a conclusion that is not
25 obvious from this patent.

1 Q. Well, so you said before that a child
2 file can inherit a placement policy from its
3 parent file; is that right?

4 A. Yes.

5 Q. And that placement policy could include
6 a restriction to a specific directory; is that
7 correct?

8 A. That's possible, but also could be --
9 how about this. How about say, hey, as a
10 placement policy, every file has to be its own
11 directory, that's it. And every file should be in
12 a different repository. Why? I won't have --
13 redundancy to survive denial of service.

14 My point is there's so many possible
15 ways to place a file, you cannot say that because
16 it's the same placement policy, they have to be
17 the same directory. No, I don't read it that way.

18 Q. No, I understand that. That was just
19 an example, right?

20 So I'm giving you an example where my
21 example placement policy is restricting that file
22 to a specific directory. And so in that
23 situation, when I make a copy of that file, that
24 copy can inherit that placement policy; correct?
25 The same placement policy?

1 ATTORNEY YUAN: Objection; form.

2 THE WITNESS: So, again, it is not
3 really clear from the patent, right?

4 So inherit a placement policy. But this
5 policy -- unless policy say, hey, I'm root A --
6 I'm file A, I'm the root, my placement policy says
7 put me in a file and all my child in the same
8 directory.

9 Okay, in that case I can see it. I can
10 see B is being put in the same directory, because
11 why? Because policy at the root says so, says
12 that every related files have to be in the same
13 directory.

14 But if the policy didn't say that
15 explicitly then I don't know. I mean, see what
16 I'm saying?

17 BY ATTORNEY LU:

18 Q. Yeah, I understand. My example is that
19 the policy is saying that.

20 A. Well. The point is that the policy has
21 to say explicitly all the child.

22 You know, let's say I'm A, I'm putting
23 /home/Wenke/documents, let's say. And the policy
24 explicitly say all my children have to be in the
25 same directory.

1 Okay, in that case then B would be
2 there. And then because B, then it is C's -- B's
3 children, then C may be also put in the same
4 directory. See what I'm saying? Mean that you
5 cannot inherit something that is not explicit.

6 Q. I was trying to say it was explicit,
7 but -- so you answered my question.

8 ATTORNEY YUAN: So it's been more than
9 an hour, so how long do you think?

10 ATTORNEY LU: Oh, sure, why don't we
11 take a break then.

12 THE WITNESS: How long you suggest?

13 ATTORNEY LU: If you want to take a
14 break, Dr. Lee -- it's up to you -- why don't we
15 take a 10-minute break if you want.

16 THE WITNESS: Yeah, 10 minutes would be
17 good. Thank you.

18 (Recess taken from 10:24 a.m. to
19 10:32 a.m.)

20 BY ATTORNEY LU:

21 Q. Welcome back, Dr. Lee.

22 During the break, did you talk to
23 anybody?

24 A. No.

25 Q. All right. Going back to Exhibit 1004,

1 the Cidon reference.

2 A. Okay.

3 Q. We're going to still be in the same
4 area we were before the break.

5 A. Okay. Okay.

6 Q. So in paragraph 212, it identifies
7 encryption as one of the policies you can define
8 on a document; right?

9 A. Yes, that's what it says. Yes.

10 Q. All right. So if we go to paragraph
11 218, on the next page, page 34 of the PDF.

12 A. Uh-huh.

13 Q. This is a little longer, but why don't
14 you read paragraph 218 through, I guess, 228 to
15 yourself, and let me know when you're done.

16 A. Okay.

17 (Witness reviews document.)

18 A. Okay.

19 Q. All right. So this portion of Cidon is
20 talking about encryption policies; is that
21 correct?

22 ATTORNEY YUAN: Objection; form.

23 THE WITNESS: So, again, where we came
24 from is that we talk about encryption is part of
25 what placement policy would do, right? That's the

1 paragraph 212. And then paragraph 218 further
2 explain what encryption/decryption, you know, can
3 be performed across multiple storage system,
4 federated virtual file system.

5 BY ATTORNEY LU:

6 Q. So in paragraph 222, it's talking about
7 uploading files to a web storage vendor like
8 Dropbox. And then it says:

9 "However, in such a case, it is not
10 possible to guarantee that files will be
11 uploaded to the storage service in an
12 encrypted form. In this case, the
13 management server monitors the encrypted
14 folders and encrypts unencrypted files
15 as they show up in special directories."

16 Did I read that right?

17 A. That's correct.

18 Q. So if I'm understanding correctly, you
19 have a user who uploads a file to Dropbox, for
20 example -- an unencrypted file to Dropbox for
21 example; right?

22 ATTORNEY YUAN: Objection; form.

23 THE WITNESS: I -- I mean, the way I
24 read 222 is that, you know, it's not talking about
25 the user should do this: "Continue to access

1 files through the device application provided by
2 the web" -- I mean, it -- I mean -- okay.

3 So really beginning of 222 says, "The
4 user continues to access the files through the
5 device applications provided by the web storage
6 vendor such as Dropbox."

7 And, yeah, sure we talk about purely the
8 file access method, okay. But then it go on to
9 say, hey, but if you want security, here's some
10 other things you need to do. So ...

11 BY ATTORNEY LU:

12 Q. And some of those other things it tells
13 you to do is you have a management server that
14 monitors the encrypted folders and encrypts
15 unencrypted files as they show up in special
16 directories; is that right?

17 ATTORNEY YUAN: Objection; form.

18 THE WITNESS: So, again, I think in 222
19 that's what it says. That's what this patent is
20 teaching, is that you can use a management server
21 to monitor the encrypted photos and encrypts
22 unencrypted files as they show up in the special
23 directories. So essentially it's explaining
24 the -- the -- the patent.

25 ///

1 BY ATTORNEY LU:

2 Q. Okay. And then if you go down to 224
3 there are several scenarios where the management
4 server will encrypt files; correct.

5 A. Yeah, so 224 talks about several
6 scenarios.

7 Q. So the first scenario in paragraph 225
8 is it will encrypt the file if "a file is found
9 in a folder which was designated by the
10 administrator as an encrypted folder."

11 Do you see that?

12 A. Well, it says:

13 "If the file is not changed for
14 specified period of time after it is
15 uploaded to the management server, its
16 metadata is extracted and it's encrypted
17 using 'friendly encryption method' to be
18 described. The encrypted file is then
19 erased from Dropbox."

20 Yeah. Yeah.

21 Q. Sorry.

22 So if I understand this correctly, so
23 the management server will look at this encrypted
24 folder. If it sees that there's an unencrypted
25 file there and if the file has not changed for a

1 specified period of time after its upload, the
2 management server will encrypt that file; is that
3 correct?

4 ATTORNEY YUAN: Objection; form.

5 THE WITNESS: It will -- it will extract
6 the metadata as well and also encrypt and then
7 erase the encrypted file.

8 BY ATTORNEY LU:

9 Q. Okay. And then 226 is another
10 scenario. We don't need to get into that one.
11 But I wanted to look at the one in 227 where it
12 says:

13 "Similar to (a) but a specific file
14 was found to be under the encryption
15 policy, as defined by the file ancestry
16 tree. This means that the original
17 parent is encrypted and the policy
18 dictates that all descendent files must
19 be encrypted too."

20 Do you see that?

21 A. That's what it says, yes.

22 Q. So am I right that this is saying there
23 is an encryption policy -- or there can be an
24 encryption policy where, if an original parent is
25 encrypted, then that requires all of its

1 descendent files to also be encrypted; is that
2 correct?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: Well, I think this give
5 you a scenario where the policy dictates something
6 like -- dictates, like -- 227 is saying is that,
7 you know, this means that the original parent is
8 encrypted and the policy dictates that all
9 descendent files must be encrypted too.

10 So I think what it says is that you
11 could -- I mean, you can have such a policy.

12 BY ATTORNEY LU:

13 Q. And this policy is based off of an
14 ancestry tree; right?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: Well, I think this policy
17 we talk about here -- so, again, if I read 227
18 again, it says:

19 "Similar to (a) but a specific file
20 was found to be under the encryption
21 policy as defined by the file ancestry
22 tree. This means that the original
23 parent is encrypted and the policy
24 dictates that all descendent files must
25 be encrypted too."

1 I think what this says is that you could
2 have a policy, and the policy says, hey, this
3 policy is for -- is defined for the file ancestry
4 tree. And, more specifically, you know, when the
5 file is encrypted, when the original parent is
6 encrypted, all the descendents must be encrypted
7 too, yeah.

8 So you could have -- I think what 227 is
9 saying is that you can have such a specific
10 policy.

11 BY ATTORNEY LU:

12 Q. So when it refers to "file ancestry
13 tree," that's the same ancestry tree we were
14 talking about earlier; right?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: I assume it is, but you
17 know -- yeah. I assume it is referring to the
18 ancestry tree that, for example, paragraph 195
19 provides a definition sort of, yeah.

20 BY ATTORNEY LU:

21 Q. Okay. And actually if you go back --
22 sorry.

23 Okay. So this whole section, I guess
24 I'm not -- I need some clarification on the steps.
25 Maybe you could provide it. Especially for -- as

1 described in 222 and 225.

2 So you have like a Dropbox folder that's
3 designated as -- that can be designated as an
4 encrypted folder; is that right?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: Let me see, 222.

7 (Witness reviews document.)

8 THE WITNESS: I think 222 -- sorry. 222
9 says "special directories." I do not see the
10 word -- okay.

11 And then they say -- and then it's going
12 to say "secure folders." Folders that include
13 files that should be encrypted.

14 Yeah. So I think what this says is that
15 you can -- files in this kind of either special
16 folders or folders that suggest, you know, they
17 should be secure, I think they may -- they -- let
18 me see. They're referring to the same thing? Let
19 me see.

20 (Witness reviews document.)

21 THE WITNESS: So I think really the way
22 I see is that 225 actually try to explain 222 in
23 slightly more -- in slightly clearer way.

24 BY ATTORNEY LU:

25 Q. Yeah.

1 A. My interpretation is that they
2 overloaded the terms, so using multiple terms, to
3 refer to a folder -- for example, 225 says, "A
4 file is found in a folder which was designated by
5 the administrator as an encrypted folder."

6 So I would expect that's the same
7 encrypted folder that's been referred at 222. And
8 then, you know, what's a special directory? You
9 know, could be within those encrypted folders -- I
10 mean, or what's a secure folder.

11 So anyway, so those are not very well
12 defined. But, in general, it seems to me that
13 they all refer to the files -- you know, those
14 places have files that should be -- should be
15 encrypted.

16 Q. Yeah.

17 A. Yes.

18 Q. I would agree. It's not a model of
19 clarity.

20 So why don't we look at 222. It
21 actually provides, in the middle of the paragraph,
22 there's a method. So [reading]: The method 300
23 may include fetching 310, a status of "secured"
24 folders -- again, another name for the folder --
25 folders that include files that should be

1 encrypted checking 320 if there is a nonencrypted
2 file in a secured folder. If so, checking of the
3 file remained unchanged for a predetermined
4 period. If so, processing the file by fetching
5 the file, extracting the file signature,
6 et cetera. And then it encrypts the file.

7 So this doesn't say where the
8 nonencrypted files comes from: Right? It just
9 appears in this secured folder; is that right?

10 ATTORNEY YUAN: Objection; form.

11 THE WITNESS: Okay. So basically --
12 first of all, whatever we just read in 222 I think
13 it explains -- the same thing was explained again
14 in 225, in using slightly different term of the
15 folder, this time calls it encrypted folder. But
16 also pretty clear it watch the file which has not
17 been changed for a while and then you encrypt it
18 and check the metadata and erase the unencrypted
19 files and so on and so forth.

20 But to your question of where the files
21 coming from, I think 122 in the beginning talks
22 about the user continues to access files through
23 the device application provided by the web storage
24 vendor, such as Dropbox.

25 So I think the point is that, you know,

1 the user may just continue to use Dropbox like it
2 is. That's how the file shows up -- yeah.

3 BY ATTORNEY LU:

4 Q. So you're saying the user uploads an
5 unencrypted file to this secured folder or
6 encrypted folder?

7 A. That's a possible scenario, yeah.

8 Q. And then -- that's possible.

9 A. And then the monitor -- keep monitoring
10 the folder. So let's put it this way.

11 If -- if everything is being uploaded by
12 the user to the folders already encrypted, then
13 it's a much easier job for the management server
14 to worry about, right.

15 So I think -- I think if you read 222
16 and sort of understand what the patent is saying
17 is that, hey, look, the user can access the files
18 through the -- let's say the application, let's
19 say from Dropbox as if nothing were going to
20 bother them, nothing is in the way, but then the
21 management server would monitor the file that
22 should be encrypted. And then after a while the
23 file has not been changed, meaning that the user
24 is not actively changing the content and because
25 the file is in that -- in that special folder or

1 secured folder, then go ahead and encrypt that and
2 then remove the -- erase the unencrypted file. I
3 mean, that's what it's talking about, I think.

4 Q. So the steps are a user uploads a file
5 to one of these secured folders; the management
6 server sees that unencrypted file in the secured
7 folder and then it checks if it was unchanged for
8 a predetermined period; it extracts the metadata;
9 it encrypts the file; and then it deletes the
10 unencrypted file; is that right?

11 ATTORNEY YUAN: Objection; form.

12 THE WITNESS: Like I said, that's one
13 scenario. That's seems to be suggested by 222.

14 Are there other scenarios that the file
15 would show up in those folders? You know, to read
16 the rest of the patent, to try to assess, but
17 that's the other -- the other scenarios. But the
18 scenario that we just discussed is one --
19 one -- you know, one possible scenario -- seems to
20 be, you know, at least in agreement with 222 and
21 225.

22 BY ATTORNEY LU:

23 Q. All right. So what about in 227, where
24 you have, quote, "a specific file was found to be
25 under the encryption policy as defined by the

1 file ancestry tree"?

2 So in that situation, is it the user
3 uploads an unencrypted file, the management server
4 says, Oh, this file is under an encryption policy
5 defined by a file ancestry tree; and then it says
6 this file was a descendent file of an encrypted
7 original parent so we are going to encrypt this
8 descendent file. Is that what 227 is saying?

9 ATTORNEY YUAN: Objection; form.

10 THE WITNESS: So 227 does not talk about
11 where the file is found. It's just basically say,
12 hey, you know, similar to A -- well, you know, so
13 maybe -- meaning that the file probably is in
14 the -- in the -- in a encrypted folder. I assume
15 that's the case.

16 You know, but it's -- it's under
17 the -- you know, so that's not very clear
18 whether -- whether the file is in the same folder
19 or not. So -- but in any case, I think, 227 talks
20 about when it comes to encryption, you just apply
21 the policy that's specific for the ancestry tree
22 that dictates that all descendent file must be
23 encrypted.

24 BY ATTORNEY LU:

25 Q. So I know it's not clear. But maybe --

1 maybe we can clear this up. I don't know. It's
2 definitely not clear.

3 But if -- you know, if the file was in
4 an unencrypted -- sorry. Let me withdraw that.

5 If the file was in an encrypted folder
6 or a secured folder, it would just be encrypted;
7 right? You wouldn't need to go to the file
8 ancestry tree encryption policy; is that correct?

9 ATTORNEY YUAN: Objection; form.

10 THE WITNESS: I mean, so the nuance is
11 that the patent doesn't talk about, right, even
12 though you say it's encrypted, then you say okay,
13 actually how? What key?

14 Those are the details that the patent
15 never talks about, but a POSITA like me would say,
16 Yeah, those are relevant.

17 For example, you can say, hey, for this
18 file or this whole ancestry tree, I use a
19 tree-specific key or tree-specific method. Those
20 are all possibles for POSITA's point of view.

21 So my point is that the policy may say,
22 hey, you know, I think, for the patent's point of
23 view is that all it cares is make sure that the
24 file is the same ancestry tree, everything the
25 same, ancestry tree will be encrypted. And what

1 it didn't say, a POSITA would probably agree, we
2 say hey, then we may apply whatever the
3 file-specific or tree-specific encryption key or
4 method. That's all possible.

5 BY ATTORNEY LU:

6 Q. Okay. So in 227, would that include a
7 scenario where a user uploads an unencrypted file
8 and then the system says, hey, this unencrypted
9 file is part of this ancestry tree which requires
10 that all the descendents be encrypted and so I'm
11 going to encrypt that?

12 Is that what's being contemplated in
13 227?

14 ATTORNEY YUAN: Objection; form.

15 THE WITNESS: I mean, I think 227
16 basically, say similar to A, which is the file
17 would show up in some folder that the service
18 monitor. That's at least we should expect, right?

19 And then the server finds A, you know --
20 you know, we should apply the ancestry tree policy
21 to this file. Why? Because we also discover
22 this -- this file belongs to this ancestry tree.
23 So we apply that policy defined by this ancestry
24 tree, which dictates that -- in this case dictates
25 that, you know, the original parent of course is

1 encrypted but also all the descendents will be
2 encrypted too. Yeah.

3 BY ATTORNEY LU:

4 Q. So you said the first step is that a
5 file shows up -- sorry -- a file would show up in
6 some folder that the service monitors.

7 Does Cidon says where that file comes
8 from? Or could it be anywhere? Or is it from
9 the user? Do you know?

10 ATTORNEY YUAN: Objection; form.

11 THE WITNESS: So I think we talk about
12 this, right? You know 222 talks about the user
13 continue to access files, so the file will show up
14 somewhere. And that's what it is. That's all the
15 patent talks about -- the patent talks about,
16 and -- let me see.

17 And maybe we should -- let me just take
18 a look at this.

19 I mean, if you're going back to, let's
20 say, 227, '28, it does talk about, you know, some
21 placement policies based on the ancestry subtree,
22 right.

23 So, again, what a parent didn't go into
24 detail is that, let's say, A is already in the
25 secure folder and then B is a child. And when you

1 upload -- you know, try to access B, upload B,
2 would B already in the directory that -- in the
3 same directory as A or not.

4 So those things are possible. So I
5 think what the patent talks about is that,
6 remember, the way we read this patent is we talk
7 about placement first based on ancestry tree --
8 subtree and then talk about encryption, right?

9 Again, you know, the policy would be
10 applied to the whole ancestry tree. So really, if
11 you do this in context, that, you know, you say
12 where the file is coming from?

13 Well, I mean, first of all, there's a
14 user action, right, acting with the application.
15 But then there also placement policy that tells
16 you where the file should be going to, right?
17 Should the file be -- for example, you know, going
18 back to -- you know, paragraph -- you know, 208,
19 209, 210, 211, 212 -- actually talks about, you
20 know, where you should place the files, what
21 access-sharing permissions, what encryption.

22 So my point is that putting all these
23 things together, you would expect that the POSITA
24 will understand that, yes, the user access the
25 file, but then the placement into the appropriate

1 folder is taken care of by the placement policies,
2 and then the monitor -- the management server will
3 monitor the secure folder.

4 Why? Because maybe the -- that's
5 determined by the access and sharing permission
6 says, hey -- all the encryption policy to say,
7 hey, this has to be encrypted, and then basically
8 encrypt the file. That's how I -- how I or a
9 POSITA will interpret the patent.

10 BY ATTORNEY LU:

11 Q. Okay. Can you explain to me how key
12 cryptography works.

13 A. Can you point me to the patent where
14 that term shows up?

15 Q. Well, so this patent keeps talking
16 about encrypting a file; right? Do you know how
17 encryption generally works?

18 A. Yes.

19 Q. Does it -- is one way to encrypt a
20 file, does it use a key?

21 A. Well, encryption by definition, you need
22 to use a key, yeah. And there are multiple ways
23 to use a key, there's all keys of keys, yeah,
24 depending on really what kind of encryption you're
25 talking about. You talking about symmetry key

1 encryption versus, you know, public key,
2 cryptography and so on and so forth. I mean,
3 that's all kinds of things, yeah.

4 Q. Right. So I understand there's, like,
5 you know, public-private key -- you know,
6 public-private key pairs --

7 A. Right.

8 Q. -- is one way you could do encryption.
9 But let's talk about, like, a very
10 simple method, where you just have one key; the
11 key is both -- both encrypts the data and decrypts
12 the data.

13 A. Okay.

14 Q. That's one way to encrypt some data; is
15 that correct?

16 ATTORNEY YUAN: Objection. Objection to
17 form.

18 THE WITNESS: Yeah, so, like I said,
19 that's one way, one encryption method, which is
20 called symmetry -- there's a whole family, many,
21 many specific algorithms. But internal we refer
22 this to -- referred this as a symmetry key
23 encryption, meaning you use same key -- I use the
24 same key for encryption and decryption.

25 ///

1 BY ATTORNEY LU:

2 Q. So when some data -- so let's talk
3 about -- you said it's a symmetry key? Is that
4 what you said?

5 A. Yeah, symmetric.

6 Q. Symmetric. Okay.

7 So in this class of encryption
8 mechanisms, you have a single key; right? And
9 then so if I encrypt some data with that single
10 key and then send the encrypted data to you, you
11 would not be able to see the contents of that data
12 unless you have that key that I encrypt it with;
13 right?

14 A. That's correct, yes.

15 Q. You would need that key to decrypt the
16 data that I sent you; correct?

17 A. That's correct.

18 Q. At least that's the ideal. If you're
19 able to decrypt it without my key, we would have
20 a big problem; right?

21 A. Exactly. If you store your key on the
22 server and the server is comprised, everything is
23 gone, yeah.

24 Q. Yeah. I'm not even talking about
25 stealing a key. If you break -- so that would be

1 considered breaking the encryption mechanism;
2 right? If you're able --

3 A. No, just giving a key -- which is
4 different from cryptoanalysis. Cryptoanalysis
5 actually break the key, meaning guessing what the
6 key is. And people can do that too -- well,
7 depending on how strong the key is. Anyway --
8 yeah.

9 Q. So there are multiple ways to -- for a
10 hacker, let's say, to try to decrypt the data.
11 One of -- probably the worst way, I would way --
12 maybe you don't agree, but I would say the worst
13 way is if the hacker breaks the encryption
14 algorithm and is able to decrypt any data without
15 the key; right?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: Like I said, there are
18 many ways to break the mechanism. But the method
19 they talk about breaking the encryption algorithm
20 so they can decrypt without knowing the key or
21 without having the key. Sure, that's the
22 ultimate, but it almost rarely happen. I don't
23 know rarely happens to understand why do they
24 deploy crypto mechanism, to be honest.

25 ///

1 BY ATTORNEY LU:

2 Q. Well, certainly it's not going to be
3 very common these days. But back in the
4 precomputer days when we had cyphers and things
5 like that, those were, you know, not too
6 difficult to break; correct?

7 ATTORNEY YUAN: Objection; form.

8 THE WITNESS: I wouldn't say cypher -- I
9 mean, of course I actually teach crypto in my
10 classes. Of course the first thing we talk about
11 is the cypher in the ancient Greek days or the
12 ancient Romans, they use that, like they shave
13 their head and whatever -- they put things on your
14 skull and then the hair grow, all kind of stupid
15 things.

16 But really, we think about it is almost
17 a joke in a sense. These things are not
18 cryptographically strong, meaning that it's
19 very -- just very easy to break, right? So --
20 yeah. So I think all the modern-day encryption
21 algorithms are pretty hard. You know,
22 mathematically or computationally to break them is
23 pretty hard.

24 BY ATTORNEY LU:

25 Q. You said ancient Greek and ancient

1 Romans.

2 A. Yes, yeah. Like ancient Greek and
3 ancient Roman. Yeah. They all use cyphers, yes.

4 Q. All right. So that was more of an
5 aside. Sorry.

6 A. Yeah.

7 Q. All right. So the idea in a modern
8 encryption system is that, if I encrypt some
9 data -- going back to the symmetry key example.
10 If I encrypt some data with a key, the idea is
11 that nobody should be able to access that data
12 unless they have the same key; right?

13 ATTORNEY YUAN: Objection; form.

14 THE WITNESS: Yes, right. So as I said
15 before, so symmetry key encryption, yeah, that's
16 the ideal, right. Without knowing what the key
17 is, we're not supposed to be able to see the
18 so-called plaintext, meaning the original data.

19 BY ATTORNEY LU:

20 Q. So let's say I have a laptop, I encrypt
21 a file, and I want to send it to you over, let's
22 say, like SFTP. Now, when I send it to you over
23 SFTP, the encrypted data goes through my
24 router -- I have a router now.

25 Now, the router is not going to be able

1 to decrypt the data either, right, unless it has
2 the key?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: Depends on how the key is
5 being negotiated. When I teach, I always tell
6 people, hey, you know, Rule Number 1: Don't use
7 manual crypto. Second, Rule Number 2, when you
8 use crypto, check with the cryptographers and make
9 sure you use it right.

10 So, I mean, the problem of going through
11 router is depending on how the key is being
12 negotiated. For example, you say, hey, when I
13 have this key to encrypt a file, beforehand I'm
14 going to call Quincy and say, Here is the key. So
15 the router has no way of knowing the key because I
16 call you and you write down the key and whatever.

17 On the other hand, you say stand away --
18 should probably, depending on how you implement
19 it, for -- let's say Alice and Bob, or we use A
20 and B, Alice and Bob, to negotiate the key. When
21 you negotiate the key, exchange information so at
22 the end, both sides can use the same key.

23 The point is that that kind of exchange,
24 when we do the key exchange, going through a
25 router. So if you're not careful, the router

1 actually remember exactly what things you are
2 exchanging, they can actually use the same key.

3 So there's actually a well-known attack
4 called man in the middle.

5 (Interruption by the court reporter
6 to clarify the record.)

7 A. So man in the middle. Meaning that your
8 router -- your router ISP exactly is a man in the
9 middle. When you try to connect from your
10 computer to a website, you go through a router.
11 So router is actually a man in the middle.

12 If so by -- in principal you can
13 intercept anything you want. The point is that
14 when you negotiate a key, that kind of exchange
15 starts with some clear text. And so basically
16 there's something that actually quotes and
17 actually can know, and like I said, I don't want
18 to go into the details -- whole extra time to
19 cover those details. The router may -- if you're
20 not careful, the router may actually end up having
21 the key. So that's -- right?

22 But again, like I said, the key has been
23 established long time ago -- for example, I call
24 you and say, hey, Quincy, look at a dictionary,
25 page this and that, line this number, and use

1 whatever the word from -- from, you know, whatever
2 position, and then change a few letters.

3 In that case, yeah, our key is
4 established by phone. Then the router has no way
5 of knowing.

6 BY ATTORNEY LU:

7 Q. So the router won't be able to decrypt
8 the data unless it has the key.

9 A. Yeah.

10 Q. And in a -- you know, old-fashioned, I
11 write down the key on a piece of paper and then
12 hand that to you, the router is not going to know
13 the key in that situation; right?

14 A. Right. Right. Right.

15 Q. But you're testifying that, in modern
16 systems where you have a system for exchanging
17 keys, the router may be able to obtain the key
18 that way?

19 ATTORNEY YUAN: Objection; form.

20 THE WITNESS: So again, like I said, it
21 really depends on how you implement or what router
22 you're using, whether the company was using -- at
23 home -- I mean, there's a whole lot of caveats. I
24 can go through a whole lecture about this.

25 Comes down to, you know, if I -- let's

1 say go to Google, right, you can HTTPS. Do you
2 worry about the router being able to read the
3 Gmail? Actually it's not, because you know what
4 Google is, you actually know it's public key. So
5 it can verify you're actually talking to only
6 Google so you would encrypt certain things only
7 Google can actually -- can actually read.

8 So even when you negotiate a key, that
9 itself can be protected by Google's public key, as
10 long as your browser -- you can trust your browser
11 to only use, only trust Google's public key.

12 BY ATTORNEY LU:

13 Q. Yeah.

14 A. Okay? Again say, okay, isn't that
15 public? Depends on if you look for
16 organization -- some organizations will force your
17 browser to trust their so-called Google public
18 key. In fact, they really tell you, hey, you work
19 for me, I am man in the middle, take it.

20 So I wouldn't trust -- I don't know -- I
21 don't know about you guys working for a law firm.
22 I wouldn't trust that your law firm's proxy would
23 not be able to read your Gmail because they can
24 pretend to be Google. They are allowed to and
25 they can force it --

1 Q. Well, there are signatures and stuff,
2 but --

3 A. Yeah, yeah, they can force your browser
4 to trust their so-called Google public key
5 certificate as the real certificate.

6 So anyway, that's too much detail.

7 Q. Well -- excuse me. Why don't we -- you
8 said a lot there. Why don't we try to clarify
9 some of the things.

10 So you're talking about a public key.
11 So that's a key pair cryptography; right?

12 A. Right.

13 Q. And so in that situation, if I want to
14 send some encrypted data to somebody, that
15 person -- let's say you; right?

16 A. Yep.

17 Q. So you would have both a public key
18 that everybody knows --

19 A. Yep.

20 Q. -- and a private key that only you
21 know; I don't even know it.

22 A. Right. Right.

23 Q. And then -- and then when I want to
24 send you encrypted data, I use your public key
25 that everybody knows to encrypt your data; and

1 then when you get that data, you use your private
2 key -- your private key to decrypt it.

3 Is that how it works?

4 A. That's one way of doing it, but I
5 wouldn't recommend it. And the reason is that
6 public key is extremely inefficient.

7 For example, if you use my public key to
8 encrypt a whole movie, I would try to kill you,
9 because for me to encrypt it, it takes forever.
10 So the extended scheme would be you use my public
11 key to -- encrypt a symmetry key and send it to
12 me --

13 Q. Okay.

14 A. -- and then use the symmetry key to
15 encrypt the movie because that's super efficient.
16 And still nobody can get the symmetric key. Only
17 I can, because only I can use my private key to
18 decrypt the symmetric key that you created and
19 encrypt it using my public key.

20 So that's a standard way of doing it.
21 But, again, the caveat is that, how do you know
22 you're using my true public key? Somebody can be
23 lying to you, and your corporate proxy can lie to
24 you.

25 So anyway, let's not go to that.

1 Q. Okay. So normally my corporate
2 proxy -- or normally my router is not lying to
3 me; right? The way we know it's your key is that
4 you use some third-party service to sign the key,
5 and I trust that third-party service; is that
6 correct?

7 A. Yeah. I mean, so this thing called
8 public key certificate, meaning that somebody
9 certifying that you are using the correct key of
10 Wenke Lee or correct key of Google.

11 But say, Who Is Verisign. These are
12 for-profit people. I mean, do you trust them?

13 So, again, you're going to the whole
14 space of so-called public key infrastructure. Why
15 is not -- I don't know, because you don't have a
16 central authority. Do you want the US government
17 to say, yeah, I guarantee that everybody at birth
18 time was given a public key-private key pair that
19 the government guarantee that's valid.

20 We don't want essentially controlled
21 scheme, and you want to distribute scheme where,
22 you know, Verisign and Microsoft and Symantec, all
23 of these are big certificate authorities, meaning
24 that they sign all kind of public keys to verify
25 that those are public keys. But, again, it is not

1 guarantee a lot of -- a lot of well-publicized
2 problems with the scheme.

3 Q. Yeah.

4 A. Okay.

5 Q. So it's not guaranteed, but ideally you
6 wouldn't want your router to be able to decrypt
7 your encrypted data; is that right?

8 A. Yes. That would be the goal, yes.

9 Q. So if your router is decrypting your
10 encrypted data, then it was -- somebody has
11 probably hacked into it and is trying to, you
12 know, steal your information; is that --

13 ATTORNEY YUAN: Objection; form.

14 THE WITNESS: Like I said, the router
15 can be man in the middle for many reasons. Like I
16 said, corporate router or proxy may do that for
17 whatever the reason they have, or a
18 government-agent state do this all the time, so on
19 and so forth.

20 So, I mean, I wouldn't say they hack
21 into the proxy. Maybe the proxy just decide that
22 that's within their ability or power to do that.
23 So who knows.

24 BY ATTORNEY LU:

25 Q. Okay. So going back to -- sorry.

1 Going back to the symmetric key example, if --
2 where we have a single key.

3 If I lose the key, I'm not going to be
4 able to decrypt any data that use that key to
5 encrypt it; right?

6 A. I mean, it depends on what you mean by
7 "lose." You lost the key, right? So meaning if
8 you forget the key or whatever the key storage you
9 place -- you delete that or you move machine unit
10 from one to the another and then you destroy your
11 old machine kind of thing.

12 But on the other hand, because of
13 symmetric key, right? So whoever you normally
14 send data to, that person may still -- I mean, I
15 hope would still have the same key. So you may
16 find a way that, hey -- you say, hey, Wei or Babak
17 or Quincy, hey, can you send me the key.

18 Q. So if I lose it, I'd have to go find
19 somebody who knew it.

20 A. Yeah.

21 Q. And if there isn't any such person,
22 then -- well, okay. So let's say we're not
23 transferring.

24 Let's say I just want to encrypt some
25 files so if somebody steals my hard drive, they're

1 not going to be able to access my data. So let's
2 say I just use a symmetric key to encrypt some
3 files on my computer and then I lose that key and
4 there's no way for me to recover it. That
5 encrypted data, I won't be able to decrypt it;
6 right?

7 ATTORNEY YUAN: Objection to form.

8 BY ATTORNEY LU:

9 Q. Ideally. Ideally.

10 A. Yeah, really again, you know, I would
11 caveat to say that, you know, some of them not
12 always -- Apple devices, there's a way that you
13 store your key or something into some other
14 places, almost like a password manager, right?
15 You put stuff in one place, then you have a master
16 password to unlock it and extract the keys that
17 you have. So it's like an iOS -- no, I think Mac
18 iOS has this Keychain thing, there's a place you
19 store a bunch of keys or you use a password to
20 retrieve those keys.

21 Now, if you say, hey, the key is
22 absolutely lost. There's no place to be found,
23 cannot remember it, yeah, in that case the data is
24 gone. I always tell my students, hey, look, if
25 you encrypt the data and the key is lost, you

1 might as well remove the file because there's
2 nothing you can do.

3 Q. So, you know, you talked about a
4 service or, I guess, an app that Mac iOS has
5 called Keychain, and that's, like, one way of
6 keeping your keys secure; right?

7 A. Well, the Keychain is secure as the
8 method that you use to unlock the Keychain, let's
9 put it that way.

10 Q. Right. But -- so it's one way to at
11 least avoid losing your key; is that correct?

12 A. I would say there's one way to -- to
13 worry about where do you put the key; and then
14 also Keychain allows iOS devices or Mac OS devices
15 to share, meaning that -- let's say you establish
16 a key somewhere, and then you say, hey, I also
17 have some on the computer that also belongs to me,
18 then they can access the same key.

19 That's more or less -- in storage, you
20 know, security and kind of -- you know, yeah. So
21 provides all that kind of function. Yeah.

22 Q. But the idea of Keychain, if --
23 obviously you can't guarantee it 100 percent.
24 But the idea of Keychain is to keep your key
25 secured so that some other person is not able to

1 obtain your key; is that right?

2 ATTORNEY YUAN: Objection; form.

3 THE WITNESS: So, again, like I said,
4 it's -- everything is as secure as whatever your
5 secret password that you use to unlock it. So, I
6 mean, that's why security all comes down to your
7 weak password -- or your fingerprint or your face,
8 which unfortunately we have deep fake.

9 But anyway, you're kind of screwed all
10 the way around. Yeah.

11 BY ATTORNEY LU:

12 Q. So, for example, you know, if I wrote
13 my key down on a text file in plaintext, that
14 would -- you would probably consider that to be
15 much less secure than storing my key in Mac OS
16 Keychain?

17 ATTORNEY YUAN: Objection; form.

18 THE WITNESS: Again, it really depends
19 on the context, right? So -- yeah, I don't know.
20 I mean, if you store in the Mac OS Keychain but
21 then your password -- you mean your admin password
22 is super weak, yeah, I mean, that's not great,
23 right?

24 If you wrote it down on a piece of paper
25 and hide it somewhere -- I don't know -- in a pile

1 of junk in some crazy corner in your house and
2 nobody would be able to find -- I don't know which
3 one is more secure. Depends on the context.

4 BY ATTORNEY LU:

5 Q. Would you ever recommend me write down
6 my key in a text file and store it in plaintext
7 on my hard drive?

8 ATTORNEY YUAN: Objection to form.

9 THE WITNESS: So normally it's a bad
10 idea to store your key in the plaintext and put on
11 your computer, because if your computer is
12 comprised then, of course, somebody would just
13 have to look, right? So if you use SSH, you would
14 know that you actually -- you know, you should be
15 able -- how it to put it? Even access or allow
16 your key to be used, you actually have to enter a
17 password, which means your SSH key, you know, you
18 know, the private key, is supposed to be -- you
19 know -- I mean, you could put a password protect
20 it even though it's stored on your computer.

21 BY ATTORNEY LU:

22 Q. So you're saying it's a bad idea to
23 store your key in plain -- I'm sorry. Let me
24 rephrase that.

25 So you said normally it's a bad idea to

1 store your key in the plaintext and put it on your
2 hard drive.

3 Normally it's not a bad idea to store
4 your key in Mac OS Keychain, for example; right?
5 As long as you have a strong password?

6 ATTORNEY YUAN: Objection; form.

7 THE WITNESS: So, again -- yeah, I think
8 going back and forth, really depends on the
9 context, right?

10 So let's say -- let's say you use a very
11 strong password to unlock your Mac OS, then maybe
12 it's fine, you know, to put this into your
13 Keychain. I think you probably also need your
14 iCloud password to actually unlock a Keychain,
15 yeah. You need iCloud password to unlike the
16 Keychain, because the Keychain is supposed to be
17 shared within all your iCloud devices if you so
18 choose, okay?

19 So your iCloud password, normally I
20 would recommend you don't use the same password as
21 the password that you log into your computer.

22 Anyway, so comes down to a couple of
23 things. One is, like I said, in general, if that
24 piece of information is supposed to be a secret,
25 don't leave it laying around in clear text.

1 That's, like, simple, obvious Rule Number 1.

2 On the other hand, you say, okay, I have
3 to use it all the time, then of course it's
4 probably in memory or whatever. Or when you use
5 the key to decrypt something, of course the key is
6 in memory, you know, in some sort of a clear text
7 form. And then you have to do all kinds of things
8 to make sure that other programs -- meaning that
9 other than your decryption now going to a lot of
10 programs can access it, so on and so forth.

11 So really depends on a lot of context
12 when you say what's a good idea, what's a bad
13 idea, and really also a lot of trade-off
14 situation, right?

15 So let's say, for example, server, you
16 know, you can monitor what kind of access requests
17 to the server, right? A user would not -- just a
18 regular, random user would not just be able to log
19 into a server and then look around. That's not,
20 you know, normally not happening, yeah.

21 BY ATTORNEY LU:

22 Q. All right. So earlier you said there
23 are multiple ways -- you know, there's multiple
24 algorithms for symmetric keys.

25 Are there multiple algorithms for

1 public-private key-pair cryptography?

2 A. Yeah. Yeah, everything has multiple.

3 Yes.

4 Q. So if I have an encrypted file, I would
5 need to know what algorithm was used to encrypt
6 that file; correct?

7 ATTORNEY YUAN: Objection; form.

8 THE WITNESS: Again, depends. Some of
9 the encryption schemes, part of the standard, they
10 actually put in the header or heading, whatever
11 crap, so that data, when you look at the data, the
12 header, that tells you, you know, what algorithm
13 is being used. So that's also possible. Meaning
14 that you don't have to say, oh, I use AES-256.
15 Damn, it's already in the header. You should know
16 that.

17 So -- so, again, it depends on how the
18 algorithm is implemented or do they follow some
19 kind of industry standard. For example, PKI,
20 public key, they have a standard too, so ...

21 BY ATTORNEY LU:

22 Q. So what about encrypting a file? Is it
23 normal to -- like, files don't have headers, do
24 they? Like an encrypted file, does that have a
25 header that indicates what encryption algorithm

1 it used?

2 ATTORNEY YUAN: Objection; form.

3 THE WITNESS: Quite possible -- so,
4 again, quite possible. You know, completely
5 doable. Again, it really depends on, you know,
6 what standard they want to use or whether they
7 choose to implement it or not, yeah.

8 I mean, almost every file has some kind
9 of header that tells you what's the format, you
10 know, that kind of thing, yeah.

11 BY ATTORNEY LU:

12 Q. Right. But are you -- are you aware of
13 any file system, for example, that encrypts files
14 and indicates, within that encrypted file, what
15 encryption algorithm it used?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: I mean, not off the top of
18 my head. But definitely they allow all kind of
19 header or information that we know that is by
20 design or by standard.

21 For example, if I encrypt the word
22 "hello," every single time -- let's say I say
23 "hello" and "hello" again, and each time I
24 encrypt, the encrypted result should not be the
25 same. Okay?

1 So basically, when you shift it over,
2 you have to shift what we call the initial vector
3 meaning, here's some random thing I put in there
4 to make the result different. So by -- so my
5 point is there are things that are not, you know,
6 obvious to outsiders, but the POSITA would
7 understand that we do certain things, you know, in
8 the implementation to improve security and to
9 defeat analysis, that kind of thing, yeah.

10 BY ATTORNEY LU:

11 Q. What are some common encryption
12 mechanisms for encrypting a file?

13 A. So I mentioned AES. I mean, it stands
14 for Advanced Encryption Standard. I think that's
15 the most popular one now. I mean, I think Intel
16 actually put it into their chips.

17 And there's other things. You know,
18 some of the so-called, sim cyphers, CBCs and other
19 kind of thing, cypher block -- yeah.

20 So anyway, there are quite a few of
21 them, yeah.

22 Q. So if I have a Word document and then I
23 use AES to encrypt it and then I sent you that
24 encrypted document, are you going to be able to
25 tell that I use AES to encrypt it?

1 ATTORNEY YUAN: Objection; form.

2 THE WITNESS: So, again, I would
3 double-check, but I -- I think more likely than
4 not it will be -- I would be able to -- to tell.

5 BY ATTORNEY LU:

6 Q. Do you know what -- how do you know how
7 you're able to tell?

8 A. Like I said, there's some header
9 information, some other parameters, that kind of
10 thing.

11 Q. Okay.

12 A. Yeah. So, again, like I said, I have to
13 basically spend time reading the standard again.
14 I mean, I -- you know, I'm not in the industry or
15 the vendors that supply these kind of commercial
16 products. But we talk about this in textbooks,
17 that's pretty well understood that -- why do you
18 think there's a standard organization out there,
19 even though the algorithm has been published for
20 so long. So obviously talk about these kind of
21 things. Basically, compatibility.

22 You know, you send something over there,
23 then they automatically figure out, hopefully --
24 but sometimes they actually -- when they
25 negotiate -- A and B negotiate or agree upon the

1 encryption algorithm so that there's no surprise.

2 But I'm also -- I can imagine there's
3 some vendors say, Well, why do I have to -- most
4 of them in a round of negotiations so you know
5 what algorithm I'm going to use, why don't you
6 just include that information when I send it over
7 so you don't have to guess. I mean, that's common
8 sense stuff, okay. So nothing rocket science
9 here. So anyway ...

10 ATTORNEY LU: So I'm going to move on to
11 another topic, but do you want to take a break
12 before I do that?

13 THE WITNESS: Okay, yeah, sure.

14 (Luncheon recess taken from 11:30
15 a.m. to 12:02 p.m.)
16
17
18
19
20
21
22
23
24
25

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

- - -
P R O C E E D I N G S
- - -

CONTINUED EXAMINATION

BY ATTORNEY LU:

Q. Are you ready to go back?

A. Before we start, I want to clarify a few things, that --

Q. Do you want it on the record?

A. Yes, before I forget, yes.

Q. Okay. Why don't you go ahead and make those clarifications.

A. Yeah, I think first is that I noticed in my declaration we had the priority date of the '678 patent wrong. I forgot where I saw it. I think somewhere I used the date year as 2018, which is not correct, because the --

Oh, yeah, okay. On page 10 of my declaration -- I think it's paragraph 33.

Q. Uh-huh.

A. I said I -- so, I mean, towards the end of paragraph 33, I said I presume a priority date of the '678 patent to be May 10th, 2018, and

1 that was -- that was wrong.

2 In fact, I think, the patent first page
3 talks about -- I mean, listed priority date -- I
4 think we should have used December 2nd, 2013.

5 Q. Okay.

6 A. So that was a typo.

7 Q. Yeah. All right.

8 A. Okay. That's Number 1.

9 Number 2 is I refer to all this change
10 regarding different encryption methods and keys
11 and so on and so forth. I mean, first of all, I
12 wish our discussion was more in the context of the
13 patent and then we can point to that and discuss
14 how they use encryption and, you know, and so on
15 and so forth.

16 But, you know, we started as almost a
17 general background kind of a discussion, so I want
18 to clarify a few things, make sure that we are
19 clear -- absolutely actually clear what I meant to
20 say.

21 I did say that there are multiple ways
22 to encrypt. I didn't want to say that you have to
23 use symmetric key or you have to use public key.
24 And whatever I -- this is my personal opinion that
25 public key is less efficient, meaning that if you

1 are going to encrypt a huge amount of data using
2 public key, that's not the most efficient way of
3 doing it. Other the people would rather use
4 symmetry key but, hey, if any patent choose to use
5 public key, I have no objection of that, no
6 problem there.

7 Second thing is that when we discuss
8 about proxy can be man in the middle and also you
9 should not trust your proxy not to be man in the
10 middle, steal your key or fool you with a
11 incorrect public key, all those things are
12 essentially common knowledge for POSITA to
13 consider that you just can't -- you know, the
14 proxy can do a -- many things.

15 But my -- another point is that when we
16 discuss how to store our key and so on, I think
17 all our discussion -- I don't remember whether we
18 explicitly talk about -- we talk about symmetry
19 key versus public key.

20 I would just say the same thing, meaning
21 that you want to -- if you put your symmetry key
22 on your computer, of course you should worry about
23 how to secure the access of that symmetry key.
24 But same goes to the public key of your public
25 key-private key pair. Because if your private key

1 is being stolen, then everybody can decrypt data
2 they sent to you using the public key, right? Or
3 people remove a public key then you also in big
4 trouble too.

5 So the point is that it's well known to
6 a POSITA that key is a secret. Whereas private
7 key pair -- private key of your public key-private
8 key pair or the symmetry key, you should -- you
9 know, you should take all precaution to secure it,
10 right? And if you put it on computer, then the
11 same kind of cyber attack that comes in that can
12 steal your symmetry key can also steal your
13 private key.

14 So what I'm trying to say is that the
15 secure storage and management of your crypto key
16 applies to any encryption algorithm. That's what
17 I want to say, to make sure we're on the same
18 page. Because sometimes we go back and forth,
19 sometimes talk about symmetry keys and public key.
20 I don't want to attribute my comment to only one.

21 Q. Understood.

22 A. Yeah.

23 Q. Thank you for that clarification. Now
24 let me actually ask you this first.

25 During the break, did you talk to

1 anybody?

2 A. Nope. You gave me too long a break.
3 Half an hour, plenty of time for me to reflect.

4 Q. No -- absolutely, no, that's fine.

5 Just so I'm -- I understand correctly
6 from what you just said, the public key, that's
7 public; you don't need to secure that; right?
8 It's the private key that you said should be
9 secured; is that correct?

10 A. Well, I think in our discussion before
11 the break, I also did say that your public key is
12 supposed to be public. The problem with that is
13 how do you know the authenticity of the public
14 key. That's a big problem.

15 I put my public key on the web page,
16 how do you know that your web page has not been
17 promised, somebody, you know, changed that? So
18 that's the -- you know, so somebody claim that,
19 I'm Donald Trump, this is my public key. Who is
20 going to say that's not the case?

21 Q. Putting --

22 A. Okay, go ahead.

23 Q. Putting aside authenticity, signatures
24 and things like that, the public key is generally
25 public; that's why it's public. And then your

1 testimony that you just gave about keeping keys
2 secure, that was with respect to the private key;
3 is that right?

4 A. I mean, I would say that also applies to
5 the public part of public key. Authenticity is
6 part of the goal of security, right? So meaning
7 that, you know, how do you make public key to be
8 secure and be able to fulfill its intended
9 function? I mean, I think the public key, that
10 part has to be authenticated, and that's why
11 there's a lot of efforts -- we're not quite there
12 yet -- to try to have a way for people to be able
13 to verify that's your public key.

14 For example, I think Google and
15 Facebook, all these companies, they want to
16 publicize their public key and public
17 certificate --

18 Q. Right.

19 A. -- so that people can verify.

20 Q. So any other corrections that you had
21 to your declaration?

22 A. Those are the main points that I've
23 thought about, yeah.

24 Q. I have a cough, so pardon my
25 throat-clearing.

1 Do the terms "archiving" and "backup"
2 mean anything to you?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: Again, I rather we add the
5 proper scope to discuss. I mean, otherwise, we're
6 just talking about general computer science kind
7 of thing.

8 So, I mean, if you will, can, like,
9 point me to a patent or my declaration where I
10 talk about these terms?

11 BY ATTORNEY YUAN:

12 Q. I am just talking about general
13 computer science, but sure I can point you
14 somewhere.

15 Going back to Cidon, Exhibit 1004
16 paragraph 174. This is page 32 of the PDF.

17 A. Okay, 174, okay.

18 Q. It says in the last sentence:

19 "In order to save communication and
20 storage, a single fetch operation of a
21 new file from the storage servers to the
22 management server can be used not only
23 for DNA extraction but also for other
24 services, such as encryption analytics,
25 virus and malware filtering, archiving

1 and backup to other storage services and
2 files synchronization between services."

3 Do you see that?

4 (Witness reviews document.)

5 A. Okay, yeah, yes.

6 Q. So my question was, with respect to
7 where it says archiving and backup to other
8 storage services, what does the term "archiving
9 and backup" mean to you?

10 A. So archive really is plain, ordinary
11 meaning. You put things in a place as -- as a
12 record; and also in this case, you have probably
13 the file there as well, and you probably have a
14 log that say, hey, in this place, I have archive
15 these following files and where they are. So I
16 would consider that as an example for archive.

17 Again, different application may have
18 some other additional elements when they -- from
19 archiving.

20 Q. Go ahead.

21 A. Yeah, yeah, so that's archiving. Like I
22 said, plain, ordinary meaning.

23 Q. Sure. And what about "backup"?

24 A. So "backup" normally means that I let's
25 say put a copy of the -- of your file and some

1 kind of backup -- let's say storage -- so that if
2 you somehow, for whatever reason, lost the file,
3 you know, or corrupt it or whatever, you can go to
4 back up and retrieve the copy that's stored there.

5 Q. What's the difference between archiving
6 and backup?

7 A. I really -- like I said, I think these
8 kind of things can be dependent on the application
9 scenario. So I really can't say much -- you know,
10 I mean, I've seen multiple different kinds of ways
11 of doing archiving and backup.

12 For example, people backup multiple
13 versions of the same file so basically say, okay,
14 if you lost this file, which -- you know, what
15 time frame -- and go back to. And sometimes say,
16 well, isn't that the same thing as archiving?
17 Again really depending on is archiving a single
18 copy versus having multiple versions. Some
19 people, yeah, you should have multiple versions.

20 So, again, like I said, really depending
21 on how people interpret these terms and make it
22 specifically suitable for their -- for their work
23 requirements, let's put it that way.

24 ATTORNEY LU: Okay. Sorry. Could we
25 take a short five-minute break?

1 ATTORNEY YUAN: Okay.

2 THE WITNESS: Okay, yeah, sure.

3 (Recess taken from 12:14 p.m. to
4 12:19 p.m.)

5 BY ATTORNEY YUAN:

6 Q. So Dr. Lee, you don't have copies of
7 the prior art in front of you, the physical
8 copies?

9 A. No, I don't.

10 ATTORNEY LU: Okay. So I'm going to
11 upload Auradkar -- I don't know if that's how you
12 pronounce it, but it's Exhibit 1009.

13 (Exhibit Number 1009 was previously
14 marked for identification.)

15 BY ATTORNEY LU:

16 Q. Let me know when you have that.

17 A. Okay.

18 Q. And you're familiar with this document;
19 right?

20 A. I've read it, yes.

21 Q. And that's one of the references that
22 you rely on in your expert report?

23 A. Yes, in my declaration, I talk about
24 this, yes.

25 ATTORNEY LU: Sorry, let's look at a

1 different reference. I want to do that one first.

2 (Exhibit Number 1006 was previously
3 marked for identification.)

4 BY ATTORNEY LU:

5 Q. So I'm uploading the Shifka reference,
6 which is Exhibit 1006. Let me know when you have
7 that.

8 A. Okay.

9 Q. And you've seen this document before
10 too; right?

11 A. Yes.

12 Q. And this is also a reference that you
13 rely on in your declaration?

14 A. Yes. In my declaration, yes.

15 Q. Okay. So this is not a very long
16 reference, but some of the processors are a
17 little confusing to me.

18 So why don't we turn to paragraph 29,
19 page 7 of the PDF. And sorry it's a pretty long
20 paragraph so why don't you go ahead and read that,
21 Dr. Lee, to yourself.

22 A. Uh-huh.

23 Q. And let me know when you're done.

24 (Witness reviews document.)

25 A. Okay. I think I read it.

1 Q. Sorry.

2 So this paragraph 29, it begins with:

3 "The client 16 generates one or
4 more indexes 24 for one or more
5 documents 26 that are to be encrypted as
6 encrypted documents 14 and stored on the
7 storage providers 18."

8 And then it goes on:

9 "Each index 24 includes one or more
10 keywords for the encrypted documents 14
11 and pointers to the encrypted documents
12 14 containing the keywords."

13 Did I read that right?

14 A. Uh-huh, yes.

15 Q. Are you familiar with the concept of an
16 index?

17 ATTORNEY YUAN: Objection; form.

18 THE WITNESS: So index, of course, is
19 very overloaded term depending on where you're
20 using it. So in the context of this patent,
21 Shifka, I mean, explains why basically say each
22 index 24 contains one or more keywords for the
23 encrypted documents and pointers to the encrypted
24 documents containing the keywords.

25 That's what index means here.

1 BY ATTORNEY YUAN:

2 Q. And what is the purpose of this index?

3 A. So that I think they don't really do a
4 search for encryption -- range a search over
5 encrypted content, you can actually, you know --
6 basically be able to locate the documents that
7 contain the keywords. I mean, that's -- that's
8 what the definition of this index entails,
9 actually.

10 Q. Right. So you -- sorry.

11 You said, "That's what the definition of
12 this index entails, actually."

13 What -- would you be able to provide
14 what a definition of an index is?

15 A. In general, the index is -- I mean, it's
16 like a table index. I mean, it's like, I don't
17 know.

18 In my deposition, I'm sure you guys can
19 generate a table of index of all the words that I
20 use and which page that word show up. That will
21 be example of an index that everybody on call here
22 would understand. We seen them plenty.

23 But, you know, like I said, index is a
24 very overly used term everywhere. But what I'm
25 trying to say, in the context of Shifka patent, it

1 talks -- it says very clearly that the indexing
2 for one or more keywords for the encrypted
3 document and pointers to the encrypted document
4 that contains those keywords, right?

5 And then -- and then it goes on to say
6 that the don't -- the same paragraph, paragraph
7 29, it talks about the index can be encrypted
8 using searchable encryption mechanisms so you can
9 actually search over and say, hey, I want to look
10 for this keyword and you search it over the
11 encrypted index and say, ah, you know, that's a
12 match, and here is a pointer to the document.
13 That means that I tell you which document contains
14 the keywords that you use to search, something
15 like that.

16 Q. Okay. So you mentioned like an example
17 of an index -- not necessarily a computerized
18 index but like in the real world is like a
19 deposition transcript; right? At the end of the
20 transcript, there's a list of keywords -- it's
21 probably not a list of every word you said, but a
22 list of important words and the page and line
23 number you can find those words within the
24 transcript; is that right?

25 A. Yeah, that would be --

1 ATTORNEY YUAN: Objection; form.

2 THE WITNESS: -- an example of index,
3 yeah. I mean, in the context of, let's say
4 transcript or book or something, yes.

5 BY ATTORNEY LU:

6 Q. Right. And so the point of the index
7 in the transcript context is so you can -- you
8 know, these words are generally in alphabetical
9 order so it's pretty easy for you to just go to
10 the index and see, I want to say wherever Dr. Lee
11 said the word "document." And then you can go to
12 the index entry for "document" and find all the
13 places in the transcript you said "document"; is
14 that right?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: Yeah, I would say that's
17 an example of how index could be used for, let's
18 say, you know keyword search, you know, to find
19 where the document -- where in the document this
20 word shows up. And/or in the context of
21 everything is clear, meaning nothing is -- nothing
22 is encrypted, right?

23 So that's why you mention, you know,
24 it's organized by alphabetical order and all that,
25 because it's easy for people to look it up, and

1 there's no encryption going on here, yeah.

2 BY ATTORNEY LU:

3 Q. So in Shifka the index is similar;
4 right? You have -- it says you have keywords,
5 and then for each keyword, you have a pointer to
6 encrypted documents; is that correct?

7 ATTORNEY YUAN: Objection; form.

8 THE WITNESS: So like I said, it says
9 that:

10 "Each index 24 includes one or more
11 keywords for the encrypted documents 14
12 and pointers to the encrypted documents
13 14 containing the keywords."

14 Yeah. So basically it tells you which
15 document contains those keywords.

16 BY ATTORNEY LU:

17 Q. Right. So let's say I have a text file
18 that has the word "doctor" in it. So Shifka --
19 am I correct that Shifka is going to create an
20 index that contains the keyword "doctor," and
21 then associates that keyword with a pointer to my
22 text file?

23 A. Yeah, so again, it really depends on
24 the -- those are details of verification, meaning
25 that you have to -- you have to -- you can do what

1 we do with the transcript, that you can include
2 all the keywords that you think are important; or
3 you say, hey, for this application we only allow
4 you to search for certain keywords, whatever.

5 But the point is that you can decide set
6 of keywords that you allow people to search, and
7 then -- yes, then you create index, say, here is a
8 set of keywords I'll allow you to search and, you
9 know, and the pointers to documents that contain
10 that keywords, basically.

11 Meaning for each document. So basically
12 I think what 29 says that basically you do this
13 for each -- well, later on they say you can do
14 this for each document or one index for all
15 documents. Those are details, yeah.

16 Q. Right. So let's say I have like five
17 total files, and then three of them have the word
18 "doctor" in it.

19 Shifka says you create an index -- or
20 you could create an index where it has the keyword
21 "doctor" and then it has pointers to the three
22 files that contain that word "doctor"?

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Like I said, towards the
25 end of the -- well, towards -- towards the --

1 latter part of the paragraph 29 it says:

2 "For example, some searchable
3 encryption mechanisms may generate one
4 encrypted index per encrypted document,
5 while other searchable encryption
6 methods may generate a single encrypted
7 index for all the encrypted documents."

8 So really, you know, do we have one
9 index that say here is the keyword "doctor" and
10 here is all documents that contain the keyword
11 "doctor"; or for each document, you create index
12 for -- essentially say, hey, here are all the
13 keywords that this document has.

14 So really those are essentially details,
15 yeah. I mean, the patent -- Shifka talks about,
16 you know, all these are possible.

17 BY ATTORNEY LU:

18 Q. And what does Shifka mean by "pointer"
19 to the document?

20 A. So -- okay. So essentially -- I mean,
21 those are implementation details, right? A
22 pointer, for example, I would consider a file name
23 can be a pointer, possibly. And if later on talk
24 about the segment or can be segment ID, you know,
25 can be file ID, basically a pointer can be, hey,

1 here is a way to locate that piece of data, either
2 by part file or by whatever. I'm using file name,
3 as an example.

4 Q. You cut off a little bit, so --

5 A. So what I'm trying to say, the pointer
6 in computer science terms normally means here
7 is -- here is a -- so a pointer can mean many
8 things. I mean, strictly speaking can mean an
9 address somewhere that you can go to and find the
10 data that you want. But then also we talk about
11 file, can be the name so that you can use the
12 name, you know, as the pointer to go to your
13 storage and say, hey, I want this file, given the
14 name.

15 And sometimes name by itself may or may
16 not be sufficient. Of course, if you say this is
17 the unique name within the namespace, you know,
18 you can do that to tell the storage server here is
19 the namespace -- here is the namespace and here is
20 the unique name or pointer within the namespace.
21 Or you can say, hey, here is the full path.

22 But, again, those are implementation
23 details. All you need to know is that pointer
24 allows you to locate a file, find out where to
25 basically get the file. And also, I think, later

1 on we talk about, you know, if you -- if you
2 include segments and all that, then also, you
3 know, you could also include segment ID there too
4 there.

5 Q. So the point of being able to locate
6 the file or the segment is so that later, if I
7 want to look up the word "doctor," I could just
8 use my index, and my index will tell me, here are
9 the locations of the three files that have the
10 word "doctor"; is that right?

11 A. Actually, that's not -- that's -- so
12 that's actually -- I think -- hold on.

13 I use file name as an example. But I
14 think the declaration talks about this, that -- I
15 would say the pointer is actually the ID, meaning
16 that a way to identify that particular file or
17 particular segment; and where that file segment is
18 stored, actually there's another table that the
19 broker -- I mean, like if you look at Figure 3 or
20 so on or -- actually Figure 2 and 3 -- actually
21 Figure 1, 2 -- all the figures talk about this
22 broker in the middle that actually would maintain
23 a table that tells you where this particular, you
24 know, file or segment is being stored in terms of
25 the storage.

1 Q. Okay. So you said a lot of things
2 there. Let's try to break it down a little bit.
3 So you said that the pointer is actually
4 the ID. By "ID" you mean like an identifier;
5 right?

6 A. Yep.

7 ATTORNEY YUAN: Objection; form.

8 BY ATTORNEY LU:

9 Q. So is it your testimony that the
10 identifier itself is not enough to locate the
11 data?

12 A. So, again, identify is identify. So
13 tells you basically the naming -- naming the files
14 or naming the segment. But it's being stored,
15 actually that information is maintained by the
16 broker to say, because the same file can be stored
17 in multiple storage.

18 So -- meaning that the ID does not tell
19 you the exact path, exact path where it is, okay?
20 That's what I'm saying.

21 Hold on. I think we talk about this in
22 my -- I talk about this in my declaration. I
23 would rather go to that. Let me see.

24 So I think I find it --

25 So I think paragraph 101 of my

1 declaration on page 53 -- right. So I read it to
2 you:

3 "Shifka's index 24 include one or
4 more keywords for the encrypted document
5 14 and pointers to the encrypted
6 documents 14 containing the keywords.
7 Index 24 were then using a searchable
8 encryption algorithm to produce
9 encrypted indexes 28."

10 And so that's on -- that's on -- in
11 paragraph Shifka 29:

12 "It would have been obvious to a
13 POSITA that the pointers in paragraph 29
14 of Shifka were the same as" IDs,
15 "identifiers and that were described
16 later -- in later session of Shifka.
17 Notably, the pointers/identifiers both
18 identified the encrypted documents and a
19 search of the encrypted index would
20 essentially turn the identifiers"

21 And then, you know, a POSITA would
22 understand that the pointers essentially allow
23 you to identify the complete document within the
24 namespace and then go on and find, you know,
25 where they are.

1 So I would just say that, earlier on, I
2 use the file name as example of possible pointers.
3 But I think -- you know, I mean, it could be. I
4 mean, a file name is also an example of ID or ID
5 is an example of file name, it doesn't matter.

6 The point is that it does not --
7 according to the figured recited here, you know --
8 if we go to here in the middle, it talks about
9 Table 1, it actually tells you where each document
10 is stored. They say, D1 store in SP1, that
11 means -- SP1 stands for storage provider.

12 So the point is that D1 itself is not
13 the full path, or path of where the file is. Just
14 an ID. And the name can be some whatever string
15 that you want to create and uniquely identify that
16 file within the namespace.

17 But actually where you find it, the ID
18 itself does not tell you, okay? The broker will
19 handles putting these things into the proper
20 places and then keep up the table for it to
21 retrieve from the appropriate storage provider.

22 Q. So would you agree that in Shifka, the
23 index is a map from -- let me -- let me reask it.

24 Would you agree that in Shifka the index
25 is mapping keywords to document identifiers?

1 A. Again, I don't know what you mean by
2 "map." Basically it tells you, hey, like I said,
3 the beginning of 101 it says the "index includes
4 one or more keywords of the encrypted documents
5 and pointers to the encrypted documents that
6 containing the keywords."

7 So that's what it is.

8 Q. Right. Well, you're familiar with the
9 map data structure; right?

10 ATTORNEY YUAN: Objection; form.

11 THE WITNESS: Again, in what context?

12 Map is a very loaded term.

13 BY ATTORNEY LU:

14 Q. Well, I think in any typical
15 programming language, they're going to have some
16 standard set of libraries that include data
17 structures, and one of them is usually typically
18 called a map.

19 Are you familiar with such data
20 structures?

21 ATTORNEY YUAN: Objection; form.

22 THE WITNESS: I guarantee you is not
23 being taught in any data structure algorithm. Map
24 data structure, there's no such thing. We talk
25 about memory map. That's completely different

1 context.

2 BY ATTORNEY LU:

3 Q. Okay. So let me ask --

4 A. Map itself is not data structure, let me
5 tell you that.

6 Q. Well, let me ask it this way.

7 So Shifka says, "Index 24 includes one
8 or more keywords for the encrypted document and
9 pointers to the encrypted documents 14 containing
10 the keywords."

11 My question is: Would you understand
12 "index" to be associating the keywords with the
13 pointers?

14 ATTORNEY YUAN: Objection; form.

15 THE WITNESS: Like I said, this
16 basically says that, you know, index includes one
17 or more keywords for the encrypted document and
18 pointers to the encrypted documents containing the
19 keywords.

20 Only it says -- in the index would say,
21 here are the keywords and here are the pointers or
22 IDs to document that has this keywords. That's
23 all what it is.

24 BY ATTORNEY LU:

25 Q. Right. And so using Shifka's index I'm

1 able to say, okay, like so here is the keyword
2 "doctor" and for that keyword "doctor," here are
3 the identifiers for the documents that contain
4 that word.

5 Is that how it works?

6 A. Again, you basically have to search the
7 complete index.

8 Shifka talks about the index should be
9 encrypted using such encryption algorithms, and
10 you're going to say, hey, which document contains
11 the keyword "doctor." You basically search the
12 encrypted index because the keyword "doctor" would
13 also be encrypted in this encrypted index and then
14 will return you a bunch of identifiers.

15 And I think that's what I said in 101,
16 right? I search -- on top of page 54, I say "a
17 search of the encrypted indexes 28 returns
18 identifiers (e.g., D1, D2, D3) of the one or more
19 encrypted documents."

20 So that's in Shifka.

21 Q. And what would that search typically
22 look like in terms of the algorithm that's being
23 used?

24 ATTORNEY YUAN: Objection; form.

25 THE WITNESS: So basically go back to

1 Shifka, paragraph 36 -- no, 39. Let's see where
2 it talks about this.

3 (Witness reviews document.)

4 THE WITNESS: So basically I think
5 Shifka 36 --

6 (Incidental comments made off the
7 stenographic record.)

8 THE WITNESS: So I just briefly browsed
9 at the paragraph 36. It does provide some more
10 details.

11 But even in paragraph 29, it talks
12 about, you know -- let's see, the top of page 7 it
13 talks about, you know, encrypt -- encrypts the one
14 or more indexes using a searchable encryption
15 algorithm generating one or more encrypted
16 indexes. And then talks about, you know, the
17 searchable encryption mechanisms to increment the
18 index maybe any searchable encryption mechanisms
19 known in the art and is typically different than
20 the encryption mechanism used to encrypt the
21 document. And so on.

22 And then it then talk about a few
23 examples of searchable encryption algorithms, and
24 go on -- and it goes on to say, you know, you
25 don't have to use all the cited prior art. I

1 mean, it's well known there are plenty of
2 searchable encryption algorithms out there by
3 then -- yeah.

4 So really depends on, you know, how the
5 searchable encryption -- what is searchable
6 encryption algorithm is used. For example, can be
7 keyword-based; you could have, you know, like
8 paragraph 29 is saying that you can have one
9 gigantic index for all the files or one index per
10 file. All these are details.

11 BY ATTORNEY LU:

12 Q. So the index that Shifka describes,
13 that was not a new thing at the time of Shifka;
14 right? That's something that was well known to a
15 person of ordinary skill?

16 A. What do you mean by that? Meaning that
17 the specific index that Shifka talks about, is
18 what you mean?

19 Q. Well, it says an "index includes one or
20 more keywords for the encrypted documents and
21 pointers that the encrypted documents containing
22 the keywords."

23 That description of an index is not new;
24 right?

25 ATTORNEY YUAN: Objection; form.

1 THE WITNESS: Let me see here.

2 Yeah, I mean, I think -- I think the --
3 the idea of having the index -- a searchable index
4 where you kind of, you know, list the keywords and
5 then -- and then also list the documents that
6 contains the keywords the concept is -- you know,
7 I would say was -- was normal by then. But,
8 again, you know, there are always implementation
9 details that Shifka talks about within the context
10 of, you know, the patent.

11 BY ATTORNEY LU:

12 Q. And sure -- sorry.

13 And so that concept, you said it was
14 known. How long had it been known, by 2014, the
15 date of this Shifka patent?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: So I don't know people use
18 the term "index" or not. Could be, but would they
19 describe the same way as Shifka saying that here's
20 a table that list all these things and -- and you
21 should encrypt the index and on. That, I don't
22 know.

23 But in general, like I said, having some
24 way to, you know, say here are the list of
25 keywords or content and also the pointers or IDs

1 of documents that contains that, that's -- that's
2 a well-known concept.

3 Let me see whether Chiueh talks about
4 that as well.

5 Let me see whether it talks about index
6 as well.

7 Yeah, so I would say that if you look
8 at Chiueh -- I think I reference the patent -- I
9 talk about Chiueh's patent on page 120, paragraph
10 229.

11 So I basically say -- 229 says:

12 "Chiueh also disclosed creating an
13 index (e.g., significant word set (SWS))
14 that mapped encrypted keywords to
15 corresponding document ID(s) of the
16 encrypted pages, so that the concept of
17 the encrypted pages could be searched
18 using those keywords."

19 BY ATTORNEY LU:

20 Q. And the date of Chiueh is 2011; right?

21 A. Yeah, I lost track all those dates but,
22 again, you know, Chiueh -- let me see.

23 Am I allowed to bring up Chiueh on my --

24 Q. You can do whatever you want, but --

25 A. From my folder? I just want to

1 double-check what you said is correct, that the --

2 Yeah, December 20- -- yeah.

3 Q. All right. So go --

4 A. 2011, yeah. 2011, yes.

5 Q. Sorry for interrupting.

6 A. Yeah.

7 Q. So going back to this concept of a
8 searchable index, it was known by 2011 too;
9 right?

10 A. In general, searchable encryption is
11 known for a long time, and it's evident by Shifka
12 and Chiueh -- at least these are two examples that
13 we know, by around 2010ish, you know, that the,
14 you know, using -- you know, using index or
15 significant word set so that we allowed users to
16 search encrypted document using keywords. Seems
17 to me by then it's very well known and well
18 practiced.

19 Maybe -- I think before that people only
20 talk about -- by definition, searchable encryption
21 you have to have a way for people to actually
22 search. Most -- you know, very often people use
23 keyword to search, right? So creating some kind
24 of index or reference set, you know, seems to be
25 a -- I would -- I would say that it is very well

1 documented or practiced idea.

2 Q. So creating some kind of index or
3 reference set would you say was something that
4 was known in the '90s?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: So like I said, searchable
7 encryption has a long history. I haven't looked
8 specifically in the 90s, do they create index or
9 call it a index or call it a significant word set.
10 I mean, I haven't done that.

11 But, you know, for the purpose of this
12 case, right, given the priority date of the '678
13 patent is 2013, I providing some prior art, prior
14 to that date, that talks about these kind of
15 ideas, so -- Shifka and Chiueh. And I'm sure he
16 also reference some papers that talks about
17 similar ideas.

18 BY ATTORNEY LU:

19 Q. Have you ever read the -- sorry. So
20 you're familiar with the Google search engine;
21 right?

22 ATTORNEY YUAN: Objection; form.

23 THE WITNESS: Well, depending on how do
24 you mean by "familiar"? I use it every day, yeah.
25 ///

1 BY ATTORNEY LU:

2 Q. And you agree it was released in 1996?

3 ATTORNEY YUAN: Objection; form.

4 THE WITNESS: Google search engine,
5 1996, either that or somewhere prior to that,
6 yeah. Yes.

7 BY ATTORNEY LU:

8 Q. This may seem out of left field.

9 Did you ever read the paper that Larry
10 Page and Sergey Brin wrote that discussed the
11 Google search --

12 ATTORNEY YUAN: Form.

13 ATTORNEY LU: Can you let me finish my
14 question?

15 BY ATTORNEY LU:

16 Q. -- that described the Google search
17 algorithm?

18 ATTORNEY YUAN: Objection; form.

19 THE WITNESS: I'm not sure I -- yeah.
20 I'm not sure first of all how it's relevant to
21 this patent, but -- this case.

22 But I would just say -- say that my
23 recollection is that we talk about it at graduate
24 school, because we're doing some web searching
25 stuff on our own. And, oh, you know, this thing

1 is called Google. I say, what's difference, how
2 different from keyword search. And they talk
3 about all these page rank algorithm and all that.

4 So I do remember reading that -- I don't
5 remember for sure I read the original workshop
6 paper they published. But definitely one of my
7 colleagues talk about this and kind of, you know,
8 explain to me why is it different from all the
9 other search engines.

10 BY ATTORNEY LU:

11 Q. And you said you did that in grad
12 school. When were you in graduate school?

13 A. '94 to '99.

14 ATTORNEY YUAN: Objection; form.

15 BY ATTORNEY LU:

16 Q. You said 1994 to 1999?

17 A. Uh-huh.

18 Q. All right. I mean, this is definitely
19 not relevant. But I was in college from 2000 to
20 2004, and I read it then as well for one of --
21 the search engine class I took. So -- and I
22 recall that they do talk about using an index,
23 like a specialized kind of an index for page rank
24 count.

25 Anyways, that's all an aside.

1 But you would agree that, you know, the
2 concept of an index or a keyword index that was
3 very well known and has been around for many
4 decades; right?

5 A. Yeah, like I said, "indexes" are very
6 loaded term, right? Indexes is for you to find
7 relevant information depending on the kind of
8 attribute you're looking for, right? That's what
9 it is.

10 Definitely I could imagine, you know,
11 web search, you know, even the keyword base thing,
12 you could argue keyword-based stuff has some, you
13 know, way that you locate the documents that had
14 that keywords.

15 Yeah, I mean, in that sense, like I
16 said, "index" is a loaded term. But going back to
17 this case -- I mean, I think both Shifka and
18 Chiueh talks about index or significant world set
19 in a very specific context.

20 So I mean that they talk about
21 specifically, you know, the encrypted document has
22 these kind of keywords, right. So it's very
23 different from, let's say, a web search engine or
24 the table index where it's a clear text thing.
25 Meaning that a -- you know, this -- I could tell

1 you, the clear text keywords and where to find it,
2 whereas in the context of Shifka and Chiuek they
3 talk about the keywords are in encrypted
4 documents, also provides a pointers ID to those
5 encrypted documents, but then the index itself is
6 also encrypted and you can only search over that
7 encrypted index using, you know, essentially all
8 these -- whatever mechanism that the searchable
9 encryption mechanism will provide.

10 So is it different from, you know, the
11 ordinary Google's whatever crazy significant
12 search engine at the time because those index if
13 you want to call it is in clear text, and we're
14 not talking about clear text index, actually.
15 Because both Shifka and I think -- and -- talks
16 about encrypted -- encrypted index.

17 Q. Okay. So going back to Shifka, at
18 paragraph 29 on the left happened column, near
19 the bottom it says:

20 "The client 16 encrypts the one on
21 more documents 26 using any desired
22 encryption mechanism known in the art to
23 provide the encrypted documents 14."

24 Do you see that?

25 A. Okay, yes.

1 Q. And so that could include any of the
2 encryption mechanisms you testified earlier?

3 ATTORNEY YUAN: Objection to form.

4 THE WITNESS: So, again, this says that
5 basically "16 encrypts one or more documents using
6 any desired encryption mechanism known in the art
7 to provide the encrypted documents."

8 Really it says any "desired encryption
9 mechanism." I mean, that's another way of saying
10 it really depends on the application, depending on
11 your needs, whatever. I mean, that's what it
12 says, actually. Yeah.

13 So basically it's another way of saying
14 that they are teaching actually independent of
15 the specific encryption algorithm that you choose
16 to use.

17 BY ATTORNEY LU:

18 Q. So the index is independent of the
19 specific encryption algorithm for a document?

20 A. So, again, if you read what they say
21 about index, right, index talks about -- here the
22 keywords -- here the -- here the IDs or pointers
23 to the encrypted documents that has the keywords.
24 So that -- you know, I mean, really that index
25 itself when you -- you know, is basically it's

1 orthogonal to the encryption algorithm they use to
2 encrypt the documents, because this already says,
3 hey, this encrypted document has those keywords,
4 right?

5 And then, like I said, the index table
6 later on encrypted using the searchable encryption
7 algorithm.

8 Q. So Shifka is saying you have your
9 unencrypted document and then you extract out
10 some keywords to put in an index, and then you
11 encrypt that document using any desired
12 encryption mechanism, it doesn't really matter;
13 right?

14 ATTORNEY YUAN: Objection; form.

15 THE WITNESS: Basically like -- it says
16 what it says. Basically you create an index, and
17 then you say you include the algorithm using --
18 using any desired algorithm -- yeah.

19 BY ATTORNEY LU:

20 Q. Okay. The index doesn't require any
21 specific kind of encryption mechanism; right?

22 A. No. It means that -- you know, goes
23 on -- you know, the paragraph 29 goes on to say
24 that:

25 "The client encrypts the one or

1 more indexes using a searchable
2 encryption mechanism to generate one or
3 more encrypted indexes. The searchable
4 encryption mechanism used to encrypt the
5 indexes may be any searchable encryption
6 mechanism known in the art and is
7 typically different than the encrypted
8 mechanism used to encrypt the documents
9 since the searchable encryption
10 mechanism is specific to searchable
11 encryption."

12 So really what it says is not any
13 encryption algorithm but, rather, should be a
14 searchable encryption mechanism.

15 Q. Well, I'm just talking about the
16 document. I'm not talking about the index.

17 The index is, as you said, orthogonal to
18 whichever encryption mechanism you choose to use
19 for the document; right?

20 A. That's what it implies, I guess.

21 Q. So actually I wanted to see you, so as
22 you just read, it says, "Any searchable
23 encryption mechanism known in art and is
24 typically different than the encryption mechanism
25 used to encrypt the documents."

1 So this is saying, you have your
2 documents that are encrypted using one mechanism,
3 and then you have your index that is encrypted
4 using a searchable encryption mechanism; right?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: Well, that's what it says,
7 right? Those are typically different.

8 BY ATTORNEY LU:

9 Q. Do you know why they would need to be
10 different?

11 A. Because it says -- it actually says in
12 the paragraph 29, right? It says typical -- it
13 says that "it's typically different than the
14 encryption mechanism used to encrypt the documents
15 since the searchable encryption mechanism is
16 specific to searchable encryption."

17 So ... so that's the reason.

18 Q. Okay. Okay. And then if you turn to
19 paragraph 36 of Shifka, which is on the next
20 page, 8 of the PDF --

21 A. Uh-huh.

22 Q. So I don't know if you already read
23 this, but if you want to read it --

24 A. Yeah, let me read it, please. I will
25 read it.

1 (Witness reviews document.)

2 A. Okay.

3 Q. So this paragraph is talking about the
4 user sending a query and then the query
5 responding with -- using the encrypted index to
6 respond to -- sorry, let me reask that.

7 So this paragraph is talking about a
8 user who provides a query and then the system
9 retrieves the encrypted indexes and uses those
10 encrypted indexes and returns document identifiers
11 that contain the term that was used in the query;
12 right?

13 ATTORNEY YUAN: Objection; form.

14 THE WITNESS: So what it says, that
15 basically it was -- it would --

16 Yeah, so basically the broker would
17 actually first know the specific search --
18 searchable encryption algorithm that was used to
19 encrypt the specific -- to -- to uses the -- how
20 to put it -- yeah.

21 So use the specific searchable
22 encryption algorithm that would use the encrypted
23 query and the index as the input, and -- yeah.

24 And then the server only sort of -- it
25 says that only obtains the encrypted indexes for

1 that particular user, for that particular client.

2 Normally that's how it they work.

3 And then basically -- you know, and
4 then, of course, perform the search over the
5 encrypted index and get the IDs of the documents
6 that contains the words being searched and so on.
7 Yeah.

8 BY ATTORNEY LU:

9 Q. So actually:

10 "The broker server uses the
11 Translation Table T1, which is stored in
12 local memory, to look up the identifiers
13 returned by the test function (e.g., D2)
14 and then retrieves the corresponding
15 encrypted documents 14 from the storage
16 providers 18 according to standard
17 methods."

18 Right?

19 A. Let me see. Storage providers 18 --

20 Q. So I was reading from the patent.

21 A. Okay. And let me see here.

22 Yeah, so basically, I mean --

23 Yep, yep.

24 Q. And then the broker -- and then it goes
25 on, at the bottom of page 8 on the left-hand

1 side:

2 "The broker server 12 then returns
3 the retrieved encrypted documents 14 to
4 the client 16 over the first
5 communication link 20. The client 16
6 may then unencrypt the encrypted
7 documents 14 since the client 16 knows
8 the encryption that was used to
9 initially encrypt the document 26."

10 Do you see that?

11 A. Yes.

12 Q. So basically what happens is, I'm the
13 client, and I send -- I ask the broker server,
14 give me all the files that have the word
15 "doctor"; and then the broker server will use the
16 encrypted index to get document identifiers and
17 then fetch the files for me that contain that
18 word "doctor"; is that right?

19 ATTORNEY YUAN: Objection; form.

20 THE WITNESS: So I think you only -- I
21 mean, I think in the beginning of the -- of the
22 paragraph 36, right, it says that -- you know, the
23 second sentence:

24 "When the broker server receives
25 the encrypted query from the client 16,

1 the broker server 12 only obtains the
2 encrypted index 28 for that client to
3 execute the specific test function."

4 What I'm trying to say is that when you
5 search for "doctor," the broker probably -- the
6 broker according to the spec, to paragraph 36,
7 would only search the files that you have the
8 permission or you should be -- you should be
9 searching, because actually dictated by the -- you
10 know, searchable index for you.

11 So you cannot say, hey, I want to find a
12 file that contains "doctor," then also I get a
13 file that Wei owns that I'm not supposed to read.
14 So that's being taken care of by the broker,
15 according to 36.

16 Meaning that, you know, just because you
17 do a search of encryption doesn't mean that you
18 have access to all the files that contains this
19 keyword. You're still being essentially, you
20 know, governed by the access -- access right
21 policy -- to say the least, let's put it that way.

22 I mean, the document -- paragraph 36 is
23 pretty clear, right? The broker only used the
24 searchable index and put the index for that
25 client.

1 BY ATTORNEY LU:

2 Q. And so 36 is actually pretty clear
3 that, at the very last sentence it says:

4 "The client 16 may then unencrypt
5 the encrypted documents 14, since the
6 client 16 knows the encryption that was
7 used to initially encrypt the document
8 26."

9 And client 16 knows the encryption
10 because it was the one that encrypted the
11 document?

12 A. So, again, I mean, we can probably look
13 into the details of the workflow.

14 Let me see here. If you point me to
15 Shifka, we should probably talk about this in the
16 sense -- of the workflow meaning how the client
17 initiate -- meaning that --

18 So we talking about search, right?
19 So -- but we should probably talk about looking
20 into the -- looking into the patent to talk about
21 how the client put the request -- how the client
22 was involved in the storage -- how to put it? --
23 uploading the data in the first place, right?
24 We're not talking about searching downloading.
25 You know, we should probably take a look at how

1 does the patent talk about uploading.

2 Q. So the patent is talking about doing
3 this in like a system like Dropbox; right? Are
4 you familiar with Dropbox?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: I have used Dropbox, yes.

7 BY ATTORNEY LU:

8 Q. So let's say I'm a user and I uploaded
9 a document that was encrypted. I can just
10 retrieve that document and then decrypt it;
11 right? I don't need to use the search function?

12 ATTORNEY YUAN: Objection; form.

13 THE WITNESS: Can you repeat the
14 question again.

15 BY ATTORNEY LU:

16 Q. Sure.

17 So Shifka at 36 is talking about using
18 the broker server to perform a search, and then --
19 and the client will receive encrypted files it can
20 unencrypt; right?

21 A. Yes.

22 Q. Okay. And -- sorry, let me just
23 withdraw that and move on.

24 Let's see.

25 A. Yeah, I mean, just to -- I mean, if you

1 look at their figures, right, talk about multiple
2 cloud providers, right, not just Dropbox, right --
3 you know, SP1, 2, 3, 4, 5, it talks about cloud
4 providers, which means, you know, you can be
5 Dropbox, can be, you know, Google Drive whatever.

6 So Google takes care of storing it, if
7 you need to, to multiple providers. So it's not
8 just -- that's why search is actually useful. I
9 mean, all you look up Table T1, T2 are useful
10 because you don't know it's actually always in
11 Dropbox.

12 Yeah, and also if you look at Figure --
13 figures -- basically it does -- let me see.

14 Yeah, it talks about files being, you
15 know, uploaded to -- to the broker. I mean, by
16 then, I think documents, you know, would have
17 been, you know, encrypted. Index would have been
18 encrypted too, so ...

19 Q. So you said search is useful. But in
20 order to -- if I knew where an encrypted specific
21 file was located, like if I knew it was on
22 Dropbox, I could just retrieve it and then
23 unencrypt it there; right? I don't need to use
24 the search?

25 ATTORNEY YUAN: Objection; form.

1 THE WITNESS: I mean, if you -- if you
2 so choose that you only use a specific provider --
3 a specific storage server, then you have to defeat
4 the purpose of -- I would say defeat the -- you
5 know, pretty much how to put it --

6 Well, I mean, Shifka does a couple of
7 things. One is that he actually makes sure that
8 the files would be encrypted. And then -- you
9 know, before it's been loaded. So when it say
10 clients load -- loaded -- uploading the encrypted
11 data or index to the storage provider, I think we
12 talk about this, the monitor system tree, make all
13 those, you know, take place, actually monitors and
14 performs some of those functions.

15 Let me see where is that. I remember it
16 right or wrong, let me see.

17 BY ATTORNEY LU:

18 Q. I think that might have been Cidon.

19 A. Sorry, yeah. Cidon, sorry I confused --
20 conflated -- sorry. Too many prior art, actually,
21 to talk about.

22 Okay. So basically, I think, Shifka
23 talks about encryption on the client side, which
24 is fine. You encrypt that.

25 And then you upload the encrypted file

1 index to the broker, and the broker would take
2 care of, you know, putting them into multiple --
3 for security purposes can put them into different
4 providers.

5 I mean, that has significant benefits,
6 right? Meaning why would you put all -- all your
7 file into one place? So, I mean, that's -- that's
8 really -- why it would -- it would be nice for
9 the -- for the broker to perform the search for
10 you, because you don't have to know which
11 provider -- which storage provider is storing your
12 encrypted data.

13 Q. So --

14 ATTORNEY YUAN: It has been a bit over
15 an hour, excluding the five-minutes short break.
16 So how long do you plan to continue?

17 ATTORNEY LU: Why don't we take a
18 10-minute -- break?

19 THE WITNESS: Before we go off, I just
20 want to make sure I clarify, because I -- I
21 confused Cidon and Shifka for a moment.

22 Just basically, if you look at figures
23 of Shifka, it's pretty clear that the client
24 performs the encryption, and then once it gets the
25 data back, it performs the decryption. Okay.

1 So ...

2 ATTORNEY LU: Okay. Thank you.

3 ATTORNEY YUAN: Yeah, all right. Thank
4 you.

5 (Recess taken from 1:17 p.m. to
6 1:26 p.m.)

7 BY ATTORNEY LU:

8 Q. Dr. Lee, welcome back.

9 Did you talk to anybody during the
10 break?

11 A. No.

12 Q. All right. So before the break you
13 were saying that in Shifka, the encryption
14 happens on the client; right?

15 A. Uh-huh.

16 Q. Whereas in Cidon, the encryption
17 happens on the server; is that correct?

18 A. Let me see what's called --

19 ATTORNEY YUAN: Objection; form.

20 THE WITNESS: Let me see the term that
21 they used.

22 BY ATTORNEY LU:

23 Q. I think they use the term "management
24 server" performs the encryption; right?

25 A. Let me look at the figure to make sure

1 we use the right term here.

2 I kind of remember we read about
3 this -- which was it? Let me see. Which --

4 Q. So, for example, paragraph 224 of the
5 Cidon. It says, "the management server will
6 encrypt the files."

7 A. Okay, yeah.

8 Q. So actually I want to talk about it a
9 little bit. So going back to Shifka, at -- if
10 you go to paragraph 48, which is at the bottom of
11 page 9 of the PDF.

12 A. Yes.

13 Q. Could you read that paragraph and let
14 me know when you're done.

15 A. Okay.

16 (Witness reviews document.)

17 A. Yeah. Yes.

18 Q. So it says, at the bottom of page 9:

19 "The broker system 10 also ensures
20 that the broker server 12 cannot access
21 and/or discover the content of the
22 client's data because the broker server
23 12 does not know the encryption used on
24 the encrypted documents 14. Thus, the
25 broker server 10 provides searchable

1 encryption while maintaining the
2 confidentiality of data external to the
3 client 16."

4 Did I read that correctly?

5 A. Yes.

6 Q. So that's why, in Shifka, the client
7 performs the encryption; right?

8 ATTORNEY YUAN: Objection; form.

9 THE WITNESS: I'm not sure that's the
10 only reason. I mean -- I mean that's -- so can
11 you repeat the question again. I'm --

12 BY ATTORNEY LU:

13 Q. Let me reask it then.

14 That's one of the reasons why, in
15 Shifka, the client performs the encryption?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: Well, I mean, of course,
18 if the client performs encryption, then only the
19 client supposedly can decrypt encrypted data. I
20 mean, that's -- that's what it is.

21 In this case, the broker doesn't know
22 the encryption algorithm being used and the key so
23 they cannot decrypt -- decrypt the file content --
24 yeah, in that sense -- yeah. I mean, in that
25 sense, the broker, like -- the bottom of page 48

1 says, "The broker server providers searchable
2 encryption while maintaining the confidentiality
3 of the data external to the client," meaning that
4 when the data is not in the client's hand, the
5 confidentiality is still maintained.

6 Yeah, from the broker's -- I mean, from
7 the context of this patent, that statement is
8 correct, yeah.

9 BY ATTORNEY LU:

10 Q. Okay. All right. I think we can put
11 that aside for now. Why don't we turn --

12 A. Hold on. Hold on.

13 But -- but if the -- if the goal is to
14 provide confidentiality, like I said, you know,
15 there's multiple ways of doing this. Meaning, you
16 don't have to say, oh, in order to provide
17 confidentiality of the data, every single client
18 has to encrypt their own -- just like -- like
19 enterprise.

20 So enterprise, your proxy may decide to
21 basically, like what Cidon is doing, to encrypt
22 data for you, you don't have to worry about it.
23 And then is still -- the confidentiality is still
24 protected in the context of your enterprise.

25 So yeah, I mean, really -- you know, all

1 I'm trying to say is that I don't want to -- I
2 don't want to say that the only way to provide
3 data confidentiality is the -- is each client
4 encrypts his own data and no one else knows about
5 it. That's -- that's not -- that's -- in general,
6 not a statement I want to make. But Shifka does
7 talks about the client encrypts, right.

8 Q. All right. So, yeah, we can put that
9 one away. Why don't we turn -- did I upload it?
10 I uploaded Auradkar; right? Yeah, I did.

11 Exhibit 1099, Auradkar.

12 A. I have it.

13 Q. So this one is quite a bit longer than
14 the other. If you go to paragraph 128, which is
15 on page 65 of the PDF.

16 A. Okay.

17 Q. And you can read that, and let me know
18 when you're done.

19 (Witness reviews document.)

20 A. Yep.

21 Q. So Auradkar says, "A customer 1400 may
22 have various records 1402 from which at 1430,
23 encrypted indexes 1404 are generated."

24 Do you know if Auradkar describes what
25 these encrypted indexes look like?

1 ATTORNEY YUAN: Objection; form.

2 THE WITNESS: I actually have to -- let
3 me see what my declaration talks about. That will
4 be the first place I want to look.

5 BY ATTORNEY LU:

6 Q. Sure. I can point you to one place.
7 Let's say starting at paragraph 222 of your
8 calculation.

9 A. All right.

10 Q. Or more specifically 225.

11 A. Okay, let me see.

12 Okay, so 225, and then 226. And then
13 226 I reference Auradkar 130.

14 (Witness reviews document.)

15 So I talk about in my declaration
16 paragraph 225 about encrypting -- this example;
17 right?

18 You can encrypt tags for payload, such
19 as XML fragment; and a tag can include a file name
20 and so -- so that you can actually search, if you
21 want to search based on file name, you can do
22 it -- actually encrypt it -- you can perform a
23 searchable encryption because those tags would be
24 encrypted, right? So you can actually do a search
25 over that to find the encrypted file.

1 But then also in paragraph 226 of my
2 declaration, I reference Auradkar paragraph 130.

3 And then if you read the paragraph 130
4 in the Auradkar patent, it talks about -- I
5 think -- I mean, the second half of that it talks
6 about:

7 "To perform upload, document 1500
8 is encrypted, 1520 and uploaded 1530 to
9 the cloud into an encrypted document
10 store 1550. The location 1534 and the
11 key 1525 for the upload along with the
12 keywords 1510 are input into generated
13 inputted indexes associated with the
14 encrypted upload of documents and the
15 encrypted indexes generated at 1540
16 uploaded at 1545 to encrypted index
17 store."

18 So if the question is, where does
19 Auradkar talks about generating these indexes and
20 encrypt them and upload them, like I said,
21 paragraph 130 in Auradkar patent talks about that.

22 Q. And then if you turn to paragraph 138
23 of Auradkar, which is on page 66.

24 A. You say 138? Okay.

25 Q. Yeah, 138.

1 A. Uh-huh.

2 Q. And just -- if you want to go ahead and
3 read that, let me know when you're done.

4 (Witness reviews document.)

5 A. Okay.

6 Q. So it says in the middle, "As a result
7 the encrypted data and indices can now be handed
8 over to another entity that is not fully trusted,
9 such as a CSP."

10 Do you see that?

11 A. Uh-huh.

12 Q. And according to paragraph 137, a CSP
13 is a cloud service provider or operator; right?

14 A. Uh-huh.

15 Q. And then later at 138 it says, at the
16 last sentence:

17 "A CSP can apply encrypted queries
18 on the encrypted indices and return the
19 encrypted data that matches, however,
20 the CSP does not learn anything about
21 the contents of the data, the metadata,
22 the queries or the results, (unless
23 authorized by the customer)."

24 Do you see that?

25 A. Yes.

1 Q. So what this means is that the CSP is
2 not able to decrypt either the data or the index
3 unless the customer authorizes it to do that;
4 right?

5 ATTORNEY YUAN: Objection; form.

6 THE WITNESS: So, again, I don't know
7 what customer authorization means here. I mean, I
8 don't know, can you reference to anywhere else?
9 It talks about authorize by customer. What does
10 it mean? You see what I'm saying? Does it allow
11 you to decrypt or give you the key? I mean, it's
12 like -- what does that really mean, right?

13 BY ATTORNEY LU:

14 Q. Well, I'm not entirely sure either.
15 I'm not the expert, though.

16 But putting that aside, the "unless
17 authorized by the customer," according to the
18 sentence, "the CSP does not learn anything about
19 the contents of the data, the metadata, the
20 queries, or the results."

21 Does that mean it's because the CSP is
22 not able to decrypt the data or the indexes?

23 A. So if you read the 138 basically it
24 say -- okay.

25 Yeah. Basically it's -- let me see.

1 Yeah. So basically, you know -- so let
2 me read that.

3 "As a result the encrypted data and
4 indexes and can now be handed over to
5 another entity that is not fully
6 trusted, such as a CSP. Subsequent
7 selective access to the aggregated
8 encrypted data and indices can be
9 accomplished by the owner of that data,
10 the customer, sending up the encrypted
11 query to the CSP (or other authorized
12 subscribers). Hence, the CSP can apply
13 encrypted queries on the encrypted
14 indices and return the encrypted data
15 that matches, however, the CSP does not
16 learn anything about the contents of the
17 data, the metadata, the queries or the
18 results."

19 Yeah, I mean if you read all that, you
20 know, together, yeah, I agree what is being said,
21 because the data is encrypted -- indices encrypted
22 before it's being uploaded to CSP, you know. And
23 since it says the CSP is not fully trusted, I
24 imagine the keys would not be shared by the CSP,
25 right?

1 And also more, importantly, the query
2 itself is also encrypted. And the CSP is
3 executing the encrypted query on encrypted indices
4 after returning encrypted data.

5 So, I mean, everything is encrypted.
6 That the CSP has no key to actually decrypt, then
7 yeah, sure, it does not learn anything about the
8 data.

9 Q. Okay. And sorry, if you go backward to
10 paragraph 117 -- hold on, let me see.

11 Yeah, 117 which is page 64 of the PDF.

12 A. Okay, yeah.

13 Q. And if you want to read that.

14 A. Okay.

15 Q. Let me know when you're done.

16 (Witness reviews document.)

17 A. Okay.

18 Q. All right. So in this paragraph it
19 says, "Enterprise staff 522 can set enterprise
20 access policy 530."

21 Do you see that? It's near the top of
22 that paragraph.

23 A. "Enterprise staff 522 can set enterprise
24 access policy 530."

25 Q. Yeah. And then going on it says, "Some

1 of whom enterprise staff 522 can set enterprise
2 access policy 530."

3 A. Okay. Yeah, I see that.

4 Q. All right. So when it says "enterprise
5 staff," do you think that includes, like,
6 administrators?

7 ATTORNEY YUAN: Objection; form.

8 THE WITNESS: So staff -- you know,
9 "staff" can be a loaded term right. Anybody is a
10 staff, I guess.

11 Yeah, I mean, the staff can be, let's
12 say, a security officer, you know, some of
13 the -- you know -- some people in the management
14 role as well, for them to set policy. I would say
15 those are normally people who set the policy, not
16 the -- yeah.

17 BY ATTORNEY LU:

18 Q. Yeah, so there's a --

19 A. Yeah.

20 Q. I'm sorry.

21 A. Meaning someone -- someone who has
22 responsibility for setting this policy, not just
23 somebody -- meaning that for you to be able to set
24 this kind of important things, like access control
25 policy, you have to be specifically responsible

1 for that.

2 Q. Right. And so the access policy, it
3 says that it affect -- sorry. It says, next
4 line:

5 "Enterprise access policy 530 can
6 affect how data 512 stored in a data
7 container 510 of a cloud container 500
8 can be accessed, manipulated retrieved,
9 searched, et cetera."

10 And then it says:

11 "Accordingly, when users 508 of
12 data 512 attempt to access such data
13 512, various crypto access controls 514
14 guided by, but separated from,
15 enterprise access policy 530 protect the
16 data 512 from unwarranted access by
17 users 508."

18 Did I read that right?

19 A. Yes, uh-huh.

20 Q. So this paragraph is making a
21 distinction between enterprise staff and users;
22 correct?

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Well, I mean,
25 users -- well, the staff can also be users. Just

1 because you are a staff doesn't mean that you have
2 access to everything either, right?

3 Really so it's just depending on what's
4 your function. I mean, well -- you know,
5 enterprise that practice good security will
6 actually be careful about this, meaning that just
7 because it's your system doesn't mean that you can
8 do anything you want.

9 Yeah, so, anyway.

10 BY ATTORNEY LU:

11 Q. Yeah, so a responsible enterprise
12 probably would not have all of their users also
13 be enterprise staff; is that correct?

14 A. That's correct. But also, likewise,
15 doesn't mean that just because you're, let's say,
16 system admin, that means it can be anybody,
17 everybody's status. See what I'm saying? So,
18 yeah.

19 Q. No, I understand.

20 So you're saying, like, enterprise staff
21 could also be users, but it's unlikely that all
22 the users are going to be enterprise staff; is
23 that right?

24 ATTORNEY YUAN: Objection; form.

25 THE WITNESS: So, again, if -- if we

1 mean staff as system admin, then of course they
2 are not going to use the system admin.

3 (Interruption by the court reporter
4 to clarify the record.)

5 System administrators, meaning that if
6 by staff we mean system administrators, meaning
7 that people who actually manage and keep the
8 systems up, then in that case, not all users are
9 staff. But on the other hand, if staff means you
10 are a member of the enterprise, then everybody in
11 the enterprise is a staff. So really -- I mean,
12 yeah. It's ...

13 BY ATTORNEY LU:

14 Q. Okay.

15 A. Okay.

16 Q. Sure, I understand.

17 So the enterprise staff, as you said,
18 sets the policy for the enterprise. And would it
19 normally be the case that they're setting like --
20 like the policy is stored somewhere on an
21 enterprise server?

22 ATTORNEY YUAN: Objection; form.

23 THE WITNESS: So I don't know in the
24 context of this patent does it talk about storing
25 the policy or not.

1 But normally, you know, these kind of
2 policies, it has to be somewhere, right? It can
3 written on a board, it can be stored somewhere.
4 But basically people can -- you know, if the staff
5 say I'm going to set the policy access control
6 based on some policy, I mean, they have to have a
7 way to reference the policy, right? So where it's
8 be stored, in what shape or form, that I don't
9 know it's important to this patent, unless the
10 patent talks about it somewhere.

11 BY ATTORNEY LU:

12 Q. Yeah, I'm not sure if it does.

13 But -- well, so for example, let's say
14 you have an enterprise with like 100 users and
15 five enterprise staff.

16 Actually, no, let me withdraw that.

17 So -- so according to this paragraph
18 117, there are crypto access controls 514, and let
19 me just quote what it says. It says:

20 "Crypto access control 514 guided
21 by separate from enterprise access
22 policy protect the data 512 from
23 unwarranted access by users 508."

24 Do you see that?

25 A. Uh-huh.

1 Q. So also if you -- this might be a
2 little hard. But if you scroll up to Figure 5 --
3 this paragraph is talking about Figure 5 -- you
4 might be able to more easily visualize it.

5 A. Okay. So many figures in this patent.

6 Q. Let me see what page.

7 A. 36.

8 Q. Okay. So 36.

9 A. Figure 5.

10 Q. So if Figure 5 you see on the lower
11 left you have this box that says, "Enterprise
12 520," and inside it you have "enterprise access
13 policy 530" with a dotted arrow pointing to a
14 data container that contains crypto access
15 controls.

16 Do you see that?

17 A. Yeah.

18 Q. And then there is a separate box user
19 508 that interacts with data 512 that is within
20 these crypto access controls.

21 A. Uh-huh.

22 Q. Right?

23 A. Uh-huh.

24 Q. So based on paragraph 117 in this
25 figure, it looks like the enterprise staff, you

1 know, sets the access policy; the access policy
2 sets the crypto access controls; and the crypto
3 access controls are the thing that regulates
4 whether or not a user 508 can access the data
5 512. Is that correct?

6 ATTORNEY YUAN: Objection; form.

7 THE WITNESS: I think we should go back
8 to the paragraph to talk about it. Yeah, because
9 I mean -- paragraph is what?

10 BY ATTORNEY LU:

11 Q. 117.

12 A. 117? Yeah, 117.

13 I think I also talk about this in my
14 declaration. But, you know, let me -- let me see.
15 This is Auradkar. So -- let me see.

16 I believe it specifically talk about,
17 you know, how access -- how to protect sort of --
18 access does not allow -- let me see.

19 Q. Yeah, let me see, maybe I can try --

20 A. In my declaration I talk about this kind
21 of thing.

22 Okay. So let me see.

23 Q. So like paragraph 175, 176.

24 A. You mean in my declaration?

25 Q. Yeah.

1 A. Yeah.

2 Q. Or maybe paragraph 193 is better.

3 A. Yeah, I mean I were looking at that as
4 well. Let me see. Let me look at 193.

5 Q. You kind of just quote the paragraph,
6 but go for it.

7 A. I just want to make sure I would say
8 things that would be --

9 Q. Sure absolutely.

10 A. -- discussed previously so I don't have
11 conflict myself.

12 (Witness reviews document.)

13 Yeah, so -- so again, what was your
14 question again? I finished reading 193 already,
15 yeah.

16 Q. I was just trying to -- so looking at
17 193, because the figure is there too, I'm just
18 trying to confirm what the relationship between
19 all these components are.

20 So looking at both paragraph 117 and
21 Figure 5, enterprise staff manages the enterprise
22 access policy; right?

23 ATTORNEY YUAN: Objection; form.

24 THE WITNESS: Let me see what it says
25 here. It says that "Example of Figure 5, an

1 enterprise staff 522 can ... enterprise access
2 policy 530." That's what the first sentence of
3 117 says, yeah.

4 BY ATTORNEY LU:

5 Q. Yeah. And then 117 also says -- and
6 then you have these crypto access controls 514,
7 which 117 says are "guided, but separated from,
8 enterprise access policy 530 and they protect the
9 data 512 from unwarranted access by users 508."

10 A. Right.

11 Q. Looking at Figure 5, you see a dotted
12 arrow from the enterprise access policy to the
13 crypto access controls.

14 Do you see that?

15 A. Yeah, I think the arrow means it's
16 guided, by meaning that the enterprise access
17 policy guides to access controls. And that's what
18 arrow -- the dotted arrow from -- from the
19 enterprise access policy 530 to the data
20 contain -- the data -- yeah, to the -- whatever
21 they call it. To the --

22 Q. Crypto?

23 A. The crypto container 510 means.

24 Q. And then it's the crypto access
25 controls that protect the data 512 from

1 unwarranted access by user 508; right?

2 A. Yeah. So the way I see it, a POSITA
3 would agree that, look, if the access control
4 policy says, hey, this data 508 cannot access, it
5 belongs to, let's say, user 512, that's access
6 control policy, meaning that this data can only be
7 accessed by 5120. Okay? And --

8 Q. Why don't you use like 509, because the
9 data is 512.

10 A. Sorry what?

11 Q. If you look at the figure, the data is
12 512.

13 A. So data 512, then the user is -- okay.
14 And let me see.

15 Q. You can just use --

16 A. Okay. Okay. Supposed to say, hey,
17 access control policy says that this data 512
18 cannot be accessed by 508. That's access control
19 policy.

20 So which means then you use some crypto
21 mechanism -- for example, you can encrypt it using
22 a key that 508 has no way of, you know, be able to
23 get hold of, kind of thing, you know, or wouldn't
24 be able to -- to request even encrypted form of
25 the data.

1 So that's the -- I think that's what the
2 crypto access control would mean -- would -- I
3 mean, that's how I interpret it, as how the crypto
4 access control is guided by the access control.

5 Q. Okay. So I think I agree with you, but
6 let me just clarify.

7 So it's the crypto access control that
8 determines whether or not user 508 -- sorry. Let
9 me -- I don't want to use that. Let me withdraw
10 that.

11 So we first have an enterprise access
12 policy, and that says user 508 does not get access
13 to data 512. So that policy says that.

14 But it's not the policy that, you know,
15 manages the access to the data; it's the crypto
16 access controls that do that; correct?

17 ATTORNEY YUAN: Objection; form.

18 THE WITNESS: Well, so basically, as I
19 cited 117 here, right, also basically says that --
20 for example, say, "Accordingly" -- I'm reading
21 paragraph 117:

22 "Accordingly, when user 508 of data
23 512 attempt to access such data 512,
24 various crypto access controls 514
25 guided by, but separated from,

1 enterprise access policy protect the
2 data 512 from unwarranted access by
3 users 508."

4 Yeah, so basically protected
5 unwarranted access.

6 BY ATTORNEY LU:

7 Q. Yeah, so the crypto access controls
8 protects the data from 508, but it -- the policy
9 that 508 can't access that data comes from the
10 enterprise access policy; right?

11 ATTORNEY YUAN: Objection; form.

12 THE WITNESS: So I think 117 says here
13 is guided by the access -- enterprise access
14 policy 530.

15 I mean, the way I see it, and also a
16 POSITA will agree, is that these are basically
17 all, you know, policies within the policy
18 framework or the policy within the policy,
19 whatever you want to say it.

20 So basically, let's say the policy is
21 about enterprise data security or enterprise data
22 protection. There are multiple elements, right?
23 One is who can access what.

24 And then there's some other policy
25 elements -- you call it a policy or call it policy

1 within policy framework, and talks about, hey,
2 okay, then specifically for crypto, here's what we
3 need to do. So, you know, all these things are
4 necessary to fulfill the overall policy.

5 I mean, you can call them subpolicies or
6 policies within a policy framework, if you insist
7 that -- if you insist that everything has to be a
8 single policy. That's how I see it.

9 BY ATTORNEY LU:

10 Q. Right. So let's say the enterprise
11 staff wants to allow user 508 access to data 512.
12 So they would change the enterprise access policy
13 to say 508 is allowed access, and then that will
14 be, I guess, distributed to the crypto access
15 control to allow access; is that correct?

16 ATTORNEY YUAN: Objection to form.

17 THE WITNESS: Again -- right.

18 So, again, as to paragraph 117 says then
19 the crypto access control mechanisms -- crypto
20 access controls, they're guided by this, you know,
21 enterprise policy or updates the enterprise policy
22 to allow access by 508.

23 BY ATTORNEY LU:

24 Q. Okay. So -- so when it says "guided
25 by," it means it's following the policies of

1 enterprise access policy 530?

2 ATTORNEY YUAN: Objection; form.

3 THE WITNESS: It's guided by, guided by.

4 You know, just basically -- you know, it really
5 depends on -- the detail depends on really how
6 they actually implement the policy or what
7 language and format they use. But basically the
8 point is that if the enterprise access policy says
9 File A now has access, then the crypto access
10 control would basically -- basically follows that.

11 I mean, it's like what -- mean, it's like what --

12 BY ATTORNEY LU:

13 Q. Yeah, I'm just trying to make sure --
14 because the word "guided by" is not a
15 particularly strong word. I'm just trying to
16 make sure that the crypto access control can't
17 just do whatever it wants; right? It's going to
18 be following the enterprise access policy.

19 A. Yeah, it says guided by but also
20 separated from access control policy.

21 Q. Right. So the access control -- if the
22 enterprise access policy says 508 can have access
23 to data 512, the crypto access control is going
24 to give access; correct?

25 ATTORNEY YUAN: Objection to form.

1 THE WITNESS: Yeah, it would -- it would
2 make it happen, let's put it that way. It would
3 enable it in such a way that, you know, all the
4 other security protection are still there, right?
5 Meaning that is -- you know, encrypted all these
6 kind of things, yeah.

7 BY ATTORNEY LU:

8 Q. I think we're done with Auradkar. Why
9 don't we move on to Chiueh or "Chew." I'm not
10 sure how --

11 A. Yeah, we call it "Chay."

12 Q. Yeah. So I'll just upload it -- you
13 probably have it, but I'll just upload --

14 A. Yeah, I had it.

15 ATTORNEY LU: I'm just going to upload
16 it anyway. So this is Chiueh, Exhibit 1011.

17 (Exhibit Number 1011 was previously
18 marked for identification.)

19 THE WITNESS: Yeah, okay.

20 BY ATTORNEY LU:

21 Q. Okay. And then let's turn to page 8 of
22 the PDF, and we're going to be looking at
23 paragraphs 21 through 23.

24 A. Page 8, the last page; right?

25 Q. No, page 8 of the PDF. Page 2 if

1 you're looking at the page number at the top.

2 A. I see. Okay, page 2, sorry. Yeah.

3 Q. Paragraph 21 through 23.

4 A. 21 through 23, okay.

5 (Witness reviews document.)

6 A. Okay.

7 Q. All right. So I wanted to look at
8 paragraph 21, the second sentence. It says:

9 "In the step S215, the client 110
10 removes a part of words from the
11 document pages that are still not
12 encrypted to obtain a plurality of
13 significant words."

14 Do you see that?

15 A. Yes.

16 Q. So this is -- is it obtaining a
17 plurality of significant words from an
18 unencrypted file, is it doing this because it
19 cannot obtain the words if it's encrypted?

20 ATTORNEY TEHRANCHI: Objection; form.

21 BY ATTORNEY LU:

22 Q. Let me ask it this way.

23 Let's say I have deposition transcript
24 and I want to pull out all the significant words
25 from that transcript. I wouldn't be able to do

1 that if it was encrypted unless I decrypted it
2 first; correct?

3 A. That's correct.

4 ATTORNEY YUAN: Objection as to form.

5 BY ATTORNEY LU:

6 Q. Okay. And then so actually I wanted
7 you to look at paragraph 40, which is on page 10
8 of the PDF, so two pages later.

9 (Witness reviews document.)

10 A. Okay.

11 Q. Okay. In paragraph 40 it says:

12 "Each of the encrypted words in the
13 GSI is mapped to a corresponding
14 document ID, where the document ID
15 indicates an encrypted page where a
16 given word can be found."

17 Do you see that?

18 A. Is it -- where in the --

19 Q. So this is like kind of in the middle,
20 the bottom half.

21 A. I see. Each encrypted words -- okay.

22 Q. And then it actually goes on to say:

23 "The document ID is a combination
24 of a file name and a page offset in the
25 document, and the file name of the page

1 offset are combined and encrypted."

2 A. Uh-huh.

3 Q. And so earlier in paragraphs 21 through
4 23 it also says you use the file name and
5 page offset; right? So let me find exactly where
6 it says that.

7 Yeah, so paragraph 23 it says:

8 "In some embodiments the first
9 index information may include the file
10 name of a document and the page offset
11 in the document."

12 Do you see that?

13 A. Yes.

14 Q. So Chiueh is saying you build an index
15 with these significant keywords, and you also
16 have the document file name and offset which
17 elsewhere calls the document ID; is that correct?

18 ATTORNEY YUAN: Objection; form.

19 THE WITNESS: Well, it says the first
20 index information may include a file name of a
21 document and the page offset in the document.

22 BY ATTORNEY LU:

23 Q. Right. And then in paragraph 40 it
24 later calls this file name and page offset a
25 document ID; right?

1 A. Let me see here.

2 Okay, yeah.

3 Q. Are you with me?

4 A. Well, it says that:

5 "Where document ID indicates an
6 encrypted page where given word can be
7 found. The document -- the document ID
8 is combination of a file name and a page
9 offset in the document, and the file
10 name and page offset are combined and
11 encrypted."

12 Q. So Chiueh builds an index that contains
13 these important or significant words and a
14 document ID; correct?

15 ATTORNEY YUAN: Objection; form.

16 THE WITNESS: Can you repeat your
17 question again.

18 BY ATTORNEY LU:

19 Q. So let me just ask it this way.

20 This is pretty similar to the index in
21 Shifka; right?

22 ATTORNEY YUAN: Objection; form.

23 THE WITNESS: In what way?

24 BY ATTORNEY LU:

25 Q. Both of these indexes have keywords,

1 and both of them have document identifiers; isn't
2 that correct?

3 A. I think Shifka does not specifically
4 talks about file name, just ID, right? ID could
5 be example of file name, but I think Chiueh
6 explicitly talks about file name and offset.

7 Q. But Shifka does use -- he calls it an
8 identifier but doesn't specify what kind of
9 identifier; correct?

10 A. Yeah, basically -- yeah, ID, yeah.
11 Basically ID is a name, yeah. You can say ID is a
12 name, yeah. Yeah.

13 Q. And in Chiueh, Chiueh says the
14 identifier includes the file name and the page
15 offset?

16 ATTORNEY YUAN: Objection; form.

17 THE WITNESS: Chiueh, I think, in
18 paragraph 23 talks about the first -- in some
19 embodiment the first index information may include
20 a file name of the document and a page offset in
21 the document.

22 So it's saying that at least -- that's
23 some -- one example of index information.

24 BY ATTORNEY LU:

25 Q. And the page offset is the page within

1 the document that contains the keyword; correct?

2 Let me just give an example.

3 So if I have a document and on page 9 it
4 has the word "doctor," and I'm creating this
5 index, according to Chiueh, it's going to extract
6 out that word "doctor" and then associate it with
7 a document ID that includes the file name and the
8 page offset, which is page 9 in this case.

9 Is that correct?

10 ATTORNEY YUAN: Objection; form.

11 THE WITNESS: Yeah, so I would just
12 caution you to say that -- in the beginning of 23,
13 it talks about:

14 "After step S220, a step S225 is
15 executed, by which the client 110
16 records the encrypted significant words
17 and a plurality of information in a
18 significant word set --"

19 Yeah, so basically do this for every
20 single word.

21 "-- where the first index
22 information indicate a page in the
23 encrypted pages where the encrypted
24 significant words comes from."

25 Yeah. So the example they gave, how is

1 it different from the example that Chiueh actually
2 gave at the end of the paragraph 223, right, talks
3 about, you know, the file name AA has five pages,
4 and the significant word "home" is extracted from
5 the third page. So -- then the index -- first
6 index would have, you know, the significant word
7 of "home," and includes AA comma 3.

8 BY ATTORNEY LU:

9 Q. Chiueh doesn't specify what encryption
10 mechanism it uses; is that correct?

11 ATTORNEY YUAN: Objection; form.

12 THE WITNESS: Let me look at -- look at
13 the figure. I'm sure it talks about encryption,
14 but whether it uses specific -- has to be specific
15 encryption algorithm, that I don't recall.

16 BY ATTORNEY LU:

17 Q. But a POSITA would understand Chiueh's
18 index could use -- at least with respect to the
19 document that is encrypted, it's agnostic to the
20 encryption method; right?

21 A. Hold on, hold on. Let me see here.

22 Yeah, so if you read paragraph 8.

23 Q. Uh-huh.

24 A. And it talks about, you know, basically:

25 "The disclosure provides the

1 document processing method which is
2 described as follows: A client device,
3 this one document of plurality document
4 pages and individually encrypts --
5 encrypts the document pages by a first
6 key to obtain a plurality of encrypted
7 pages, the client removes part of words
8 from document pages, obtain plurality of
9 significant words and individually
10 encrypts a significant words by a second
11 key, different from -- different to the
12 first key to obtain a plurality of
13 encrypted significant words."

14 Yeah, so at least talks about using
15 different keys to encrypt keywords versus the
16 original document.

17 Q. Right. So why does it use different
18 keys to encrypt the keywords and encrypt the
19 document?

20 A. Well, then, there's -- could be what the
21 search encryption algorithm is asking for; and
22 also that's all kind of thing that you talk
23 about -- I mean, the academics will talk about how
24 they not leak information -- yeah.

25 So basically you don't want to -- to

1 allow people to basically say, oh, let's say the
2 keyword is encrypted using same key as the
3 document, then you can't do, just say, oh, I know
4 that this document has this word.

5 The other words I don't know, but I know
6 it has this word, because the same encrypted
7 result. So you don't want that happen. Basically
8 that's leaking something that you don't want to
9 leak.

10 So in crypto ideally you want to leak
11 nothing. That's why you use a different key, then
12 you don't even know what this document contains,
13 actually.

14 Q. Okay. So it says to use different
15 keys, but it doesn't specify which encryption
16 mechanism you use; correct?

17 A. Yeah, let me take a look. When I first
18 talk about Chiueh in my declaration, do I -- did I
19 mention that or not?

20 In the context of the -- of this case I
21 don't know -- let me see. Let me see.

22 Chiueh does not -- let me see here.

23 So it talks about this CSP key. It
24 doesn't really explain what CSP key is. Let me
25 see here.

1 Q. Yeah, I don't think it specifies what
2 kind of key it is, but it's just the key that
3 encrypts the document pages.

4 A. Yeah, I talk about -- I think the way to
5 talk about encryption, actually you separate the
6 document into pages and encrypt it, and then every
7 single -- encrypt the page individually. So I'm
8 sure there's some -- some way of doing this in
9 terms of the implementation; but if your question
10 is the specific encryption algorithm, I'm
11 trying -- I'm still trying to find where do they
12 talk about it or not talk about it, basically.

13 But I would say that the encryption is
14 different in the sense they don't encrypt the
15 whole document, because they do divide up the
16 document into pages and encrypt each page. So you
17 actually having a plurality of encrypted pages
18 basically.

19 Q. Right. But the encryption algorithm
20 you use to encrypt each page, would a POSITA
21 understand that it doesn't matter, in the context
22 of Chiueh, like, which one you use?

23 ATTORNEY YUAN: Objection to form.

24 THE WITNESS: Like I said, I mean -- I
25 mean -- I'm still trying to find where Chiueh talk

1 about, you know, an example or teaching of
2 specifically algorithm to be used. But I cannot
3 find it in my declaration, and depend -- I would
4 just say that from the point of view of
5 understanding and agreeing what Chiueh is
6 teaching, the specific algorithm they use encrypt
7 the pages, this is orthogonal to what's being
8 taught in the patent, let's put it this way.

9 BY ATTORNEY LU:

10 Q. I'm sorry.

11 A. Meaning that all the pages -- the
12 document pages, they encrypt them, any encryption
13 algorithm would -- would work in the encryption
14 step, I would say.

15 Q. Okay.

16 A. Now, if Chiueh talks about it, you know,
17 we should probably, you know --

18 Q. Yeah, I don't think it does.

19 A. Yeah.

20 Q. I went through it. I don't think it
21 does. But I understand if it does, you'll
22 incorporate that.

23 ATTORNEY LU: So let me see. Actually,
24 that's all the questions I had, so I -- I pass the
25 witness.

1 THE WITNESS: Okay. All right. Thank
2 you.

3 ATTORNEY YUAN: Counsel, can we take a
4 15-minutes break?

5 ATTORNEY LU: Sure.

6 ATTORNEY YUAN: Okay.

7 (Recess taken from 2:29 p.m. to
8 3:00 p.m.)

9 ATTORNEY YUAN: I don't have any
10 question for Dr. Lee, and we can conclude this
11 deposition.

12 - - -

13 (Whereupon, at 3:00 p.m., the proceedings
14 concluded.)

15 - - -

16

17

18

19

20

21

22

23

24

25

1
2 CERTIFICATE OF SHORTHAND REPORTER
3

4 I, Gail Inghram, Registered Diplomate
5 Reporter, Certified Realtime Reporter, California
6 Certified Shorthand Reporter No, 8635, and Notary
7 Public, the officer before whom the foregoing
8 proceedings were taken, do hereby certify that
9 the foregoing transcript is a true and correct
10 record of the proceedings; that said proceedings
11 were taken by me stenographically and thereafter
12 reduced to typewriting under my supervision; and
13 that I am neither counsel for, related to, nor
14 employed by any of the parties to this case and
15 have no interest, financial or otherwise, in its
16 outcome.

17 Dated: December 21, 2023
18

19 

20 GAIL INGRAM, BA, RDR, CRR, CA-CSR 8635
21
22
23
24
25

1 DR. WENKE LEE

2
3 RE: NETSKOPE, INC. v. FORTINET, INC.

4 December 13, 2023, DR. WENKE LEE

5 The above-referenced transcript has been completed by
6 Lexitas Legal and review of the transcript is being handled
7 as follows:

8 ___ Per CA State Code (CCP 2025.520 (a)-(e)) - Contact
9 Lexitas Legal to schedule a time to review the original
10 transcript at a Lexitas Legal office.

11 ___ Per CA State Code (CCP 2025.520 (a)-(e)) - Locked .PDF
12 Transcript - The witness should review the transcript and
13 make any necessary corrections on the errata pages included
14 below, notating the page and line number of the corrections.
15 The witness should then sign and date the errata and penalty
16 of perjury pages and return the completed pages to all
17 appearing counsel within the period of time determined at
18 the deposition or provided by the Code of Civil Procedure.

19 ___Waiving the CA Code of Civil Procedure per Stipulation
20 of Counsel - Original transcript to be released for
21 signature as determined at the deposition.

22 ___Signature Waived - Reading and Signature was waived at
23 the time of the deposition.

24 ___Federal Read and Sign Requested (FRCP 30(e)(1)(B) -
25 Locked .PDF Transcript - The witness should review the

1 transcript and make any necessary corrections on the errata
2 pages included below, notating the page and line number of
3 the corrections. The witness should then sign and date the
4 errata and penalty of perjury pages and return the completed
5 pages to all appearing counsel within the period of time
6 determined at the deposition or provided by the Federal
7 Rules.

8 XXXX ___Federal Read and Sign Not Requested - Reading and
9 Signature was not requested before the completion of the
10 deposition.

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

E R R A T A

I wish to make the following changes,
for the following reasons:

Page Line

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ CHANGE: _____

REASON: _____

_____ DATE _____

DR. WENKE LEE

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

I, DR. WENKE LEE, do hereby certify:
That I have read the foregoing
deposition;

That I have made such changes in form
and/or substance to the within deposition as
might be necessary to render the same true and
correct;

That having made such changes thereon,
I hereby subscribe my name to the deposition.

I declare, under penalty of perjury,
that the foregoing is true and correct.

Executed this ____ day of
_____, 2023, at _____,
(city)
_____.
(State)

DR. WENKE LEE

Exhibits	56:25 106:15	1400 153:21	1996 132:2,5	217 50:3,6
Ex 1002 Previous Marked 3:10 6:6 22:14	1006 110:2,6	1402 153:22	1999 133:16	218 57:11,14 58:1
Ex 1004 Previous Marked 3:15 42:13,15 56:25 106:15	1009 109:12,13	1404 153:23	1:17 149:5	222 58:6,24 59:3, 18 64:1,6,8,22 65:7,20 66:12 67:15 68:13,20 72:12 154:7
Ex 1006 Previous Marked 3:18 110:2,6	101 120:25 123:3 125:15	142 43:2,18	1:26 149:6	223 181:2
Ex 1009 Previous Marked 3:21 109:12,13	1011 174:16,17	1430 153:22	2	224 60:2,5 150:4
Ex 1011 Previous Marked 3:24 174:16,17	1021 23:6	15-minutes 186:4	2 31:23 32:3,23 33:10 80:7 101:9 119:20,21 146:3 174:25 175:2	225 60:7 64:1,22 65:3 66:14 68:21 154:10,12,16
(	109 53:17	150 25:8	20 142:5	226 61:9 154:12, 13 155:1
(2004) 31:21	1099 153:11	1500 155:7	20- 130:2	227 61:11 62:6,17 63:8 68:23 69:8, 10,19 71:6,13,15 72:20
(a) 61:13 62:19	10:24 56:18	1510 155:12	2000 133:19	228 57:14
0	10:32 56:19	1520 155:8	2001 24:8	229 129:10,11
0 31:23 32:3,23 33:10	10th 100:25	1525 155:11	2004 133:20	23 174:23 175:3,4 177:4,7 179:18 180:12
00458 9:9	110 175:9 180:15	1530 155:8	2007 24:3,4	24 111:4,9,22 115:10 121:3,7 124:7
1	117 159:10,11 164:18 165:24 166:11,12 167:20 168:3,5,7 170:19, 21 171:12 172:18	1534 155:10	2007/2008 23:25	26 25:23 111:5 135:21 142:9 144:8
1 31:23 32:4,23 33:10 80:6 94:1 101:8 119:21 122:9	11:30 99:14	1540 155:15	2008 23:5 24:2,3, 20,22 25:22	28 72:20 121:9 125:17 143:2
1.1 30:8	12 142:2 143:1 150:20,23	1545 155:16	2010ish 130:13	29 110:18 111:2 113:7 116:12 117:1 121:11,13 126:11 127:8 135:18 137:23 139:12
10 43:23 56:16 100:20 150:19,25 176:7	120 129:9	1550 155:10	2011 129:20 130:4,8	2:29 186:7
10-minute 56:15 148:18	122 66:21	16 111:3 135:20 136:5 142:4,5,7, 25 144:4,6,9 151:3	2013 101:4 131:13	2nd 101:4
100 90:23 164:14	128 31:23 32:3,23 33:10 153:14	161 11:5	2014 128:14	3
1002 6:6 22:14	12:02 99:15	174 106:16,17	2018 100:18,25	3 119:19,20 146:3 181:7
1004 42:13,15	12:14 109:3	175 166:23	2023 5:1	300 65:22
	12:19 109:4	176 166:23	206 49:24 50:5,14	
	13 5:1	18 111:7 141:16, 19	207 50:19	
	130 154:13 155:2, 3,21	191 43:23 44:1,3 45:3	208 73:18	
	135 42:20	192 45:3 48:5,15, 21	209 51:22 52:1 73:19	
	137 156:12	193 45:3,17 46:10 48:6,16 167:2,4, 14,17	21 174:23 175:3,4, 8 177:3	
	138 155:22,24,25 156:15 157:23	194 45:3 48:6,16 49:3,7	210 52:1 73:19	
	14 22:17 111:6,10, 12 115:11,13 121:5,6 124:9 135:23 141:15 142:3,7 144:5 150:24	195 44:1 45:7 46:14 48:18 63:18	211 52:1 73:19	
		1990s 21:18	212 52:1 57:6 58:1 73:19	
		1994 133:16	213 50:1	

310 65:23	172:11 173:23	9:10 5:1	actively 67:24	181:15 182:21
32 106:16	5120 169:7		add 32:13 106:4	184:10,19 185:2,6,13
320 66:1	514 161:13	A	addition 44:4	algorithms 75:21
33 100:21,24	164:18,20 168:6 170:24	a.m. 5:1 56:18,19 99:15	additional 107:18	78:21 94:24,25 125:9 126:23 127:2
34 57:11	520 165:12	AA 181:3,7	address 19:21 118:9	Alice 80:19,20
36 126:1,5,9 139:19 142:22 143:6,15,22 144:2 145:17 165:7,8	522 159:19,23 160:1 168:1	ABCD 32:6,22 33:13,19	admin 91:21 162:16 163:1,2	allowed 33:19 83:24 129:23 130:15 172:13
39 126:1	53 121:1	ability 87:22	administrator 60:10 65:5	alphabetical 114:8,24
3:00 186:8,13	530 159:20,24 160:2 161:5,15 165:13 168:2,8,19 171:14 173:1	absolutely 89:22 101:19 104:4 167:9	administrators 160:6 163:5,6	Amazon.com 25:2
4	54 125:16	academic 47:6	Advanced 97:14	amount 102:1
4 146:3	6	academics 182:23	AES 97:13,23,25	analysis 97:9
40 176:7,11 177:23	64 159:11	access 52:3 58:25 59:4,8 66:22 67:17 72:13 73:1,24 74:5 79:11 89:1 90:18 92:15 94:10,16 102:23 143:18,20 150:20 158:7 159:20,24 160:2, 24 161:2,5,12,13, 15,16 162:2 164:5,18,20,21,23 165:12,14,20 166:1,2,3,4,17,18 167:22 168:1,6,8, 9,12,13,16,17,19, 24 169:1,3,4,5,17, 18 170:2,4,7,11, 12,15,16,23,24 171:1,2,5,7,9,10, 13,23 172:11,12, 13,14,15,19,20,22 173:1,8,9,16,18, 20,21,22,23,24	AES-256 95:14	analytics 106:24
41 22:18,22	65 153:15		affect 161:3,6	ancestors 50:21
42 22:17 23:11 31:17 37:8 38:16 39:7	66 155:23		affirmed 5:7	ancestry 41:10, 23 43:3,8,19 44:14,17 45:10 46:15 47:22 50:17,25 51:13 61:15 62:14,21 63:3,12,13,18 69:1,5,21 70:8,18, 24,25 71:9,20,22, 23 72:21 73:7,10
48 150:10 151:25	678 6:1,12 7:7,17, 20 8:7,25 10:25 41:22 100:17,25 131:12		aggregated 158:7	ancient 78:11,12, 25 79:2,3
493 24:8,13	7 110:19 126:12		agnostic 181:19	and/or 114:20 150:21
5	8		agree 31:11 49:19 65:18 71:1 77:12 98:25 122:22,24 132:2 134:1 158:20 169:3 170:5 171:16	app 90:4
5 23:1,7,18 24:5,6 146:3 165:2,3,9, 10 167:21,25 168:11	7 110:19 126:12		agreeing 185:5	appears 66:9
500 161:7	8 42:21 139:20 141:25 174:21,24, 25 181:22		agreement 68:20	Apple 89:12
508 161:11,17 164:23 165:19 166:4 168:9 169:1,4,18,22 170:8,12,22 171:3,8,9 172:11, 13,22 173:22	9		ahead 10:5 44:7 68:1 100:13 104:22 107:20 110:20 156:2	application 13:19 14:4 15:11, 22 16:16,17,18 48:25 49:2 59:1 66:23 67:18 73:14 107:17 108:8 116:3 136:10
509 169:8	9 150:11,18 180:3, 8	access-sharing 73:21	album 40:17,18	application- specific 49:6,13
510 161:7 168:23	90s 131:4,8	accessed 161:8 169:7,18	algorithm 77:14, 19 95:5,12,18,25 96:15 98:19 99:1, 5 103:16 121:8 123:23 125:22 126:15 127:6 132:17 133:3 136:15,19 137:1, 7,17,18 138:13 140:18,22 151:22	
512 161:6,12,13, 16 164:22 165:19 166:5 168:9,25 169:5,9,12,13,17 170:13,23 171:2	94 133:13	accomplished 158:9		
	941 6:14,25 7:7, 11,21,22 8:9	acting 73:14		
	99 133:13	action 73:14		

applications 17:10 59:5	18 20:8,11 21:3,9, 10,15 22:4 26:1, 15,23 27:1,4,7,12, 18,23,24 28:1,3, 10,12,13 29:2,5,8, 11,25 30:1,5,10, 12,14,17 31:5,14 32:9,16 33:16,22 39:25 40:2,12,21 41:3,8,11,13,19 42:5,17 43:15,21 44:23 45:6,23 46:11 48:3,20 50:13,18 51:24 52:5,12,21 53:9, 10 55:1,17 56:8, 10,13,20 57:22 58:5,22 59:11,17 60:1 61:4,8 62:3, 12,15 63:11,15,20 64:5,24 66:10 67:3 68:11,22 69:9,24 70:9 71:5, 14 72:3,10 74:10 75:16 76:1 77:16 78:1,7,24 79:13, 19 80:3 82:6,19 83:12 87:13,24 89:7,8 91:2,11,17 92:4,8,21 93:6 94:21 95:7,21 96:2,11,16 97:10 98:1,5 99:10 100:7 106:3,11 108:24 109:1,5, 10,15,25 110:4 111:17 112:1 114:1,5,15 115:2, 7,16 116:23 117:17 120:7,8 123:10,13,21 124:2,14,24 125:24 127:11,25 128:11,16 129:19 131:5,18,22 132:1,3,7,12,13, 15,18 133:10,14, 15 136:3,17 137:14,19 139:5,8 140:13 141:8 142:19 144:1 145:5,7,12,15 146:25 147:17 148:14,17 149:2, 3,7,19,22 151:8, 12,16 152:9 154:1,5 157:5,13 160:7,17 161:23 162:10,24 163:13, 22 164:11 166:6, 10 167:23 168:4 170:17 171:6,11 172:9,16,23 173:2,12,25 174:7,15,20 175:20,21 176:4,5 177:18,22 178:15, 18,22,24 179:16, 24 180:10 181:8, 11,16 184:23 185:9,23 186:3,5, 6,9	attorneys 10:4 attribute 103:20 134:8 Auradkar 109:11 153:10,11,21,24 154:13 155:2,4, 19,21,23 166:15 174:8 authenticated 105:10 authenticity 104:13,23 105:5 authorities 86:23 authority 86:16 authorization 157:7 authorize 157:9 authorized 156:23 157:17 158:11 authorizes 157:3 automatically 98:23 avoid 90:11 aware 96:12 B B's 56:2	Baback 25:10 Babak 10:12,14 88:16 back 8:12 31:16 56:21,25 63:21 72:19 73:18 78:3 79:9 87:25 88:1 93:8 100:8 103:18 106:15 108:4,15 125:25 130:7 134:16 135:17 148:25 149:8 150:9 166:7 background 101:17 backup 106:1 107:1,7,9,23,24 108:1,6,11,12 backward 159:9 bad 92:9,22,25 93:3 94:12 Balakrishnan 31:20 32:1,8 bar 19:7,21 base 134:11 based 31:1 50:16 62:13 72:21 73:7 154:21 164:6 165:24 basic 15:5 basically 13:5 18:1 23:12 30:16 37:19 38:16 39:14 43:18 47:3 49:4 51:9,20,25 66:11 69:11 71:16 74:7 81:15 97:1 98:13, 21 108:13 111:21 112:6 115:14 116:10,11,12 117:25 118:25 120:13 123:2 124:16 125:6,11, 25 126:4 129:11 136:5,13,25 137:15,16 140:15, 16 141:3,22 142:12 146:13 147:22 148:22 152:21 157:23,25 158:1 164:4 170:18,19 171:4, 16,20 173:4,7,10 179:10,11 180:19 181:24 182:25 183:1,7 184:12,18 basics 9:17 basis 27:24 begin 8:6 14:19 beginning 23:11 36:19 39:7 59:3 66:21 123:3 142:21 180:12 begins 111:2 belong 25:16 46:15 47:22 48:17 belongs 71:22 90:17 169:5 benefits 148:5 Bi 46:8 big 76:20 86:23 103:3 104:14 birth 86:17 bit 35:7 46:7 118:4 120:2 148:14 150:9 153:13 block 97:19 board 164:3 Bob 80:19,20 book 114:4 bother 67:20 bottom 135:19 141:25 150:10,18 151:25 176:20 box 165:11,18 break 35:6 56:11, 14,15,22 57:4 76:25 77:5,18 78:6,19,22 99:11 103:25 104:2,11 108:25 120:2 148:15,18 149:10, 12 186:4
-----------------------------------	---	--	--

breaking 77:1,19	calls 66:15 177:17,24 179:7	checks 68:7	clarity 65:19	178:10
breaks 77:13	care 74:1 143:14 146:6 148:2	Chew 174:9	class 76:7 133:21	comma 181:7
briefly 126:8	careful 40:14 80:25 81:20 162:6	child 41:17 43:13, 17 44:22 45:1,2,5, 21 46:10,23 47:7, 12 48:1,14 51:8 54:1 55:7,21 72:25	classes 78:10	comment 103:20
Brin 132:10	carefully 46:19	children 45:8 55:24 56:3	clean 5:25 6:1 8:22	commented 11:22
bring 7:10 129:23	cares 70:23	chips 97:16	cleaner 8:15	comments 126:6
broadly 31:7	case 24:19 27:21 38:20 41:25 42:4 47:18 55:9 56:1 58:9,12 69:15,19 71:24 82:3 89:23 104:20 107:12 131:12 132:21 134:17 151:21 163:8,19 180:8 183:20	Chiueh 129:3,8, 12,20,22,23 130:12 131:15 134:18 174:9,16 177:14 178:12 179:5,13,17 180:5 181:1,9 183:18,22 184:22,25 185:5, 16	clear 55:3 66:16 69:17,25 70:1,2 81:15 93:25 94:6 101:19 114:21 134:24 135:1,13, 14 143:23 144:2 148:23	commercial 98:15
broker 119:19,22 120:16 122:18 140:16 141:10,24 142:2,13,15,24 143:1,5,6,14,23 145:18 146:15 148:1,9 150:19, 20,22,25 151:21, 25 152:1	cases 7:6 8:3	Chiueh's 129:9 181:17	clearer 64:23	common 31:1 78:3 97:11 99:7 102:12
broker's 152:6	catch 8:20	Chiuek 135:2	client 111:3 135:20 137:25 141:1 142:4,5,7, 13,25 143:2,25 144:4,6,9,16,21 145:19 147:23 148:23 149:14 151:3,6,15,18,19 152:3,17 153:3,7 175:9 180:15 182:2,7	commonly 22:25
browse 20:2	caution 9:24 180:12	choose 93:18 96:7 102:4 136:15 138:18 147:2	client's 150:22 152:4	communication 10:3 106:19 142:5
browsed 126:8	caveat 85:21 89:11	chosen 31:22 32:20	clients 147:10	companies 20:19 105:15
browser 19:21, 22 20:1,5,20,25 26:17 28:18 83:10,17 84:3	caveats 82:23	Cidon 41:23 42:7 53:11 57:1,19 72:7 106:15 147:18,19 148:21 149:16 150:5 152:21	cloud 25:2 146:2, 3 155:9 156:13 161:7	company 82:22
build 177:14	CBCS 97:18	cite 23:6	colleagues 133:7	compatibility 98:21
builds 178:12	central 86:16	cited 126:25 170:19	collection 31:18	complete 121:23 125:7
bunch 11:2 25:18 89:19 125:14	certificate 84:5 86:8,23 105:17	claim 104:18	collectively 25:15,16	completely 47:17 96:4 123:25
C	certifying 86:9	clarification 63:24 103:23	client's 150:22 152:4	components 167:19
C's 56:2	cetera 34:2 66:6 161:9	clarifications 100:14	clients 147:10	comprised 76:22 92:12
calculate 49:5	change 82:2 101:9 172:12	clarify 26:16 81:6 84:8 100:9 101:18 148:20 163:4 170:6	cloud 25:2 146:2, 3 155:9 156:13 161:7	computationally 78:22
calculation 154:8	changed 60:13, 25 66:17 67:23 104:17	cited 126:25 170:19	colleagues 133:7	computer 81:10 89:3 90:17 92:11, 20 93:21 102:22 103:10 106:6,13 118:6
call 25:16 33:21 36:20 47:25 80:14,16 81:23 97:2 112:21 131:9 135:13 168:21 171:25 172:5 174:11	changing 67:24	claim 104:18	collection 31:18	computerized 113:17
called 24:7 29:7 35:15,18,19 50:11 75:20 81:4 86:7 90:5 123:18 133:1 149:18	chat 27:20	clarification 63:24 103:23	college 133:19	concept 16:16 111:15 128:6,13 129:2,16 130:7 134:2
	Chay 174:11	clarifications 100:14	colon 19:25	Concepts 30:8
	check 66:18 80:8	clarify 26:16 81:6 84:8 100:9 101:18 148:20 163:4 170:6	column 17:5 25:4 26:4 49:22 135:18	conclude 186:10
	checked 22:2		columns 16:11 17:5	concluded 186:14
	checking 66:1,2		combination 176:23 178:8	
			combined 177:1	

conclusion 53:24	163:24 183:20 184:21	178:14 179:2,9 180:1,9 181:10 183:16	cryptographers 80:8	144:23 147:11 148:12,25 150:22 151:2,19 152:3,4, 17,22 153:3,4 156:7,19,21 157:2,19,22 158:3,8,9,14,17, 21 159:4,8 161:6, 12,16 164:22 165:14,19 166:4 168:9,19,20,25 169:4,6,9,11,13, 17,25 170:13,15, 22,23 171:2,8,9, 21 172:11 173:23
conditions 45:4 48:7,8,12,14	continue 58:25 67:1 72:13 148:16	corrections 105:20	cryptographicall y 78:18	database 12:16, 18,19 13:7,24 14:7,9,11,22,23, 24,25 15:2,15,17, 20,25 16:10,23
confidentiality 151:2 152:2,5,14, 17,23 153:3	CONTINUED 100:6	correctly 17:14 58:18 60:22 104:5 151:4	cryptography 74:12 75:2 84:11 95:1	databases 14:20 15:13
confirm 167:18	continues 59:4 66:22	corrupt 108:3	CSP 156:9,12,17, 20 157:1,18,21 158:6,11,12,15, 22,23,24 159:2,6 183:23,24	date 12:9 25:21 47:10 100:16,18, 24 101:3 128:15 129:20 131:12,14
conflated 147:20	control 52:3 160:24 164:5,20 169:3,6,17,18 170:2,4,7 172:15, 19 173:10,16,20, 21,23	cough 105:24	current 35:11 37:3	dated 45:18 47:11 48:10
conflict 167:11	controlled 86:20	counsel 12:6 27:24 30:1 186:3	customer 153:21 156:23 157:3,7,9, 17 158:10	dates 129:21
confused 35:22 147:19 148:21	controls 161:13 164:18 165:15,20 166:2,3 168:6,13, 17,25 170:16,24 171:7 172:20	counsels 10:10	customized 15:24	day 46:7 131:24
confusing 110:17	convention 13:20	count 133:24	cut 118:4	days 78:3,4,11
connect 81:9	copied 43:4,10, 20 46:5	counted 11:21	cyber 103:11	DC 29:10,13
connection 46:4	copies 109:6,8	couple 10:16,18 93:22 147:6	cypher 78:8,11 97:19	dc:description 29:7,14 30:4
considerations 52:20	copy 5:25 6:1,9 41:14 43:12,13 45:19,21 46:1,2,5, 7 47:11,25 52:3 53:5,6 54:23,24 107:25 108:4,18	court 22:13 81:5 163:3	cyphers 78:4 79:3 97:18	decades 134:4
considered 46:22,23 77:1	corner 92:1	cover 81:19	cypto 172:19	December 5:1 101:4 130:2
constitutes 21:7	corporate 85:23 86:1 87:16	crap 95:11	D	decide 49:2 87:21 116:5 152:20
container 161:7 165:14 168:23	correct 6:5 19:3 32:8 40:1 41:2 43:14 53:12 54:7, 24 57:21 58:17 60:4 61:3 62:2 70:8 75:15 76:14, 16,17 78:6 86:6,9, 10 90:11 95:6 100:19 104:9 115:6,19 130:1 149:17 152:8 161:22 162:13,14 166:5 170:16 172:15 173:24 176:2,3 177:17	crazy 92:1 135:11	D1 122:10,12 125:18	declaration 6:1, 3,4,10 7:11,23 9:19 10:21,24,25 11:4,11,13,15,20, 22,24 22:12 31:16 100:16,21 105:21 106:9 109:23 110:13,14 119:14 120:22 121:1
contemplated 71:12		create 115:19 116:7,19,20 117:11 122:15 131:8 137:16	D2 125:18 141:13	
contemplating 52:11		created 13:10,14 43:5 85:18	D3 125:18	
content 67:24 112:5 128:25 150:21 151:23		creates 45:9	Damn 95:15	
contents 76:11 156:21 157:19 158:16		creating 129:12 130:23 131:2 180:4	data 12:20 13:8 15:15,19 16:2,4, 24,25 41:5 75:11, 12,14 76:2,9,10, 11,16 77:10,14 79:9,10,11,18,23 80:1 82:8 84:14, 24,25 85:1 87:7, 10 88:4,14 89:1,5, 23,25 95:11 102:1 103:1 118:1,10 120:11 123:9,16, 19,23,24 124:4	
context 12:11,15, 23 13:7,19,24 14:4,11,16,19 15:12 19:6 23:13, 15,20 24:1 33:25 38:18 39:8 41:25 42:3 73:11 91:19 92:3 93:9 94:11 101:12 111:20 112:25 114:3,7,20 123:11 124:1 128:9 134:19 135:2 152:7,24		cross 8:17		
		crypto 77:24 78:9 80:7,8 103:15 161:13 164:18,20 165:14,20 166:2 168:6,13,22,23,24 169:20 170:2,3,7, 15,24 171:7 172:2,14,19 173:9,16,23 183:10		
		cryptoanalysis 77:4		

154:3,15 155:2 166:14,20,24 183:18 185:3	18 108:17,20 111:19 131:23 134:7 136:10 162:3	determine 45:2,5 47:7 49:11	discussion 10:3, 10 101:12,17 102:17 104:10	183:3,4,12 184:3, 6,15,16 185:12
decrypt 76:15,19 77:10,14,20 80:1 82:7 85:2,18 87:6 88:4 89:5 94:5 103:1 145:10 151:19,23 157:2, 11,22 159:6	depends 13:19 19:5,10,13,19 40:15 80:4 82:21 83:15 88:6 91:18 92:3 93:8 94:11 95:8,17 96:5 115:23 127:4 136:10 173:5	determined 74:5	distinction 161:21	document's 39:19
decrypted 176:1	deploy 77:24	determines 170:8	distribute 86:21	documented 131:1
decrypting 87:9	deposed 6:25 9:16	device 59:1,5 66:23 182:2	distributed 172:14	documents 5:23 10:20 18:10,20 20:14 21:5 22:7 35:2 37:3,5,15,21, 22,23 38:2,7,12, 14 50:21,22 111:5,6,10,11,23, 24 112:6 115:6, 11,12 116:9,15 117:7,10 121:6,18 123:4,5 124:9,18 125:3,19 127:20, 21 128:5 129:1 134:13 135:4,5, 21,23 136:5,7,23 137:2 138:8,25 139:2,14 141:5,15 142:3,7 144:5 146:16 150:24 155:14
decryption 75:24 94:9 148:25	deposition 5:2 7:20 8:2,6 9:23 10:9 28:4 46:19 112:18 113:19 175:23 186:11	devices 89:12 90:14 93:17	divide 184:15	
decrypts 75:11	descendent 61:18 62:1,9,24 69:6,8,22	dictated 143:9	DNA 106:23	
deep 91:8	descendents 63:6 71:10 72:1	dictates 61:18 62:5,6,8,24 69:22 71:24	doable 96:5	
default 19:23,24 20:4,23	describe 128:19	dictionary 81:24	doctor 115:18,20 116:18,21,22 117:9,11 119:7,10 125:2,11,12 142:15,18 143:5, 12 180:4,6	
defeat 97:9 147:3,4	describes 127:12 153:24	difficult 78:6	document 21:13, 17 22:2,20 27:5, 20 28:16,25 29:1 30:25 34:24 35:1, 12,13,14 38:22 39:13,15 44:10 50:8,24 51:12 57:8,17 64:7,20 97:22,24 107:4 109:18 110:9,24 113:3,12,13 114:11,12,13,19 115:15 116:11,14 117:4,11,13,19 121:4,23 122:9,25 124:8,17,22 125:10 126:3,21 129:15 130:16 134:21 136:19 137:3,9,11 138:16,19 140:1, 10 142:9,16 143:22 144:7,11 145:9,10 150:16 153:19 154:14 155:7,9 156:4 159:16 167:12 175:5,11 176:9, 14,23,25 177:10, 11,16,17,21,25 178:5,7,9,14 179:1,20,21 180:1,3,7 181:19 182:1,3,5,8,16,19	
define 15:14 21:23 33:15,17 44:25 48:25 57:7	design 96:20	direct 46:2		domain 23:3 24:13
defined 30:8 31:7 32:7 33:9,14 50:20,23,24 51:12 61:15 62:21 63:3 65:12 68:25 69:5 71:23	designated 60:9 64:3 65:4	directories 25:1 51:23 53:18 58:15 59:16,23 64:9		Donald 104:19
defines 13:14 21:14 32:2	description 30:6 127:23	directory 20:2,3 25:3 34:14,15,20, 21,22 35:2,12,13, 14 36:1,7 37:5 38:7 39:16,18,23 41:6 46:21,22 52:16 53:2,22,23 54:6,11,17,22 55:8,10,13,25 56:4 65:8 73:2,3		dotted 165:13 168:11,18
defining 14:21 31:9	desired 135:21 136:6,8 137:11,18	disappear 46:25 47:3		double-check 98:3 130:1
definition 14:3 31:8 63:19 74:21 112:8,11,14 130:20	desk 6:15	disclose 10:2		download 27:22 28:14
delete 88:9	destroy 88:10	disclosed 129:12		downloading 144:24
deletes 68:9	detail 17:4 72:24 84:6 173:5	disclosure 181:25		draft 11:23 12:1,3
denial 54:13	details 10:3 17:9 21:22 70:14 81:18,19 115:24 116:15 117:14,21 118:23 126:10 127:10 128:9 144:13	discover 71:21 150:21		draw 53:24
depend 7:18 185:3		discuss 45:16 101:13 102:7,16 106:5		drive 20:1 36:17 88:25 92:7 93:2 146:5
dependent 108:8		discussed 9:6 68:18 132:10 167:10		Dropbox 58:8,19, 20 59:6 60:19 64:2 66:24 67:1, 19 145:3,4,6 146:2,5,11,22
depending 52:18 74:24 77:7 80:11,				duly 5:7

E e.g. 23:3,5 34:6 37:9,17 125:18 129:13 141:13 e.g. 31:23 34:1 earlier 63:14 94:22 122:1 136:2 177:3 earliest 45:18 easier 67:13 easiest 7:25 8:5, 10 easily 165:4 easy 78:19 114:9, 25 echo 28:7,23 efficiency 52:20 efficient 85:15 101:25 102:2 effort 12:1 efforts 105:11 eighth 29:12,14, 23,24 elements 18:13, 14,15 107:18 171:22,25 embodiment 179:19 embodiments 177:8 enable 174:3 encompasses 12:19 encrypt 60:4,8 61:2,6 66:17 68:1 69:7 71:11 74:8, 19 75:14 76:9,12 79:8,10,20 80:13 83:6 84:25 85:8,9, 11,15,19 88:5,24 89:2,25 95:5 96:21,24 97:23,25 101:22 102:1	126:13,20 128:21 137:2,11 138:4,8, 25 139:14 140:19 142:9 144:7 147:24 150:6 152:18,21 154:18, 22 155:20 169:21 182:15,18 184:6, 7,14,16,20 185:6, 12 encrypted 58:12, 13 59:14,21 60:10,16,18,23 61:7,17,19,25 62:1,8,9,23,25 63:5,6 64:4,13 65:5,7,9,15 66:1, 15 67:6,12,22 69:6,14,23 70:5,6, 12,25 71:10 72:1, 2 74:7 76:10 79:23 84:14,24 87:7,10 89:5 95:4, 24 96:14,24 97:24 111:5,6,10,11,23 112:5 113:2,3,7, 11 114:22 115:6, 11,12 117:4,6,7 121:4,5,9,18,19 123:4,5 124:8,9, 17,18 125:9,12, 13,17,19 126:15 127:20,21 129:14, 16,17 130:16 134:21 135:3,5,6, 7,16,23 136:7,23 137:3,6 138:3,7 139:2,3 140:5,9, 10,22,25 141:5,15 142:3,6,16,25 143:2 144:5,10 145:9,19 146:17, 18,20 147:8,10,25 148:12 150:24 151:19 153:23,25 154:24,25 155:8, 9,14,15,16 156:7, 17,18,19 158:3,8, 10,13,14,21 159:2,3,4,5 169:24 174:5 175:12,19 176:1, 12,15,21 177:1 178:6,11 180:16, 23 181:19 182:6,	13 183:2,6 184:17 encrypting 74:16 95:22 97:12 154:16 encryption 52:4 57:7,20,24 60:17 61:14,23,24 62:20 68:25 69:4,20 70:8 71:3 73:8,21 74:6,17,21,24 75:1,8,19,23,24 76:7 77:1,13,19 78:20 79:8,15 95:9,25 96:15 97:11,14 99:1 101:10,14 103:16 106:24 112:4 113:8 115:1 117:3,5 121:8 125:9 126:14,17, 18,20,23 127:2,5, 6 130:10,20 131:7 135:9,22 136:2,6, 8,15,19 137:1,6, 12,21 138:2,4,5,9, 11,13,14,18,23,24 139:4,14,15,16 140:18,22 142:8 143:17 144:6,9 147:23 148:24 149:13,16,24 150:23 151:1,7, 15,18,22 152:2 154:23 181:9,13, 15,20 182:21 183:15 184:5,10, 13,19 185:12,13 encryption/ decryption 58:2 encrypts 58:14 59:14,21 66:6 68:9 75:11 96:13 126:13 135:20 136:5 137:25 153:4,7 182:4,5, 10 184:3 end 7:20 11:3 19:13 36:18 80:22 81:20 100:23 113:19 116:25 181:2 engine 131:20	132:4 133:21 134:23 135:12 engines 133:9 ensures 23:13 150:19 entails 112:8,12 enter 19:1 26:19 27:9 28:17 92:16 entered 19:6 27:8 enterprise 152:19,20,24 159:19,23 160:1,4 161:5,15,21 162:5,11,13,20,22 163:10,11,17,18, 21 164:14,15,21 165:11,12,25 167:21 168:1,8, 12,16,19 170:11 171:1,10,13,21 172:10,12,21 173:1,8,18,22 entity 156:8 158:5 entry 114:12 erase 61:7 66:18 68:2 erased 60:19 essentially 12:19 13:9,23 20:24 23:18 24:18 39:4 50:15 51:16 59:23 86:20 102:12 117:12,14,20 121:20,22 135:7 143:19 establish 90:15 established 81:23 82:4 et al 22:24 31:21 everybody's 162:17 evident 130:11 exact 10:19 12:9 120:19	EXAMINATION 5:11 100:6 examined 5:9 examples 21:24 30:23 38:21 43:2, 3 52:2,4 53:16 126:23 130:12 exchange 80:21, 23,24 81:14 exchanging 81:2 82:16 excluded 32:11 excluding 148:15 exclusive 33:2 exclusively 33:2 excuse 84:7 execute 143:3 executed 180:15 executing 159:3 exhibit 6:6 22:14 23:6 27:21 28:1 42:13,15 56:25 106:15 109:12,13 110:2,6 153:11 174:16,17 exhibits 11:3 28:5 exist 35:16 exists 47:16 expect 16:13 17:4 18:11 19:22 65:6 71:18 73:23 expert 16:9 109:22 157:15 explain 13:23 14:12 23:12 30:16,18,21 34:8 51:11 58:2 64:22 74:11 133:8 183:24 explained 14:9 31:20 66:13 explaining 13:5
---	--	---	---	---

59:23	federated 58:4	16,17,24 120:16	Firefox 27:15	58:12,22 59:17
explains 66:13	fetch 106:20	122:2,4,5,13,16	firm 83:21	61:4 62:3,15
111:21	142:17	127:10 143:12,13	firm's 83:22	63:15 64:5 66:10
explicit 56:5,6	fetching 65:23	146:21 147:25	five-minute	68:11 69:9 70:9
explicitly 55:15,	66:4	148:7 151:23	108:25	71:14 72:10 75:17
21,24 102:18	field 43:1 132:8	154:19,21,25	five-minutes	77:16 78:7 79:13
179:6	figure 98:23	173:9 175:18	148:15	80:3 82:19 87:13
extended 51:2,	119:19,20,21	176:24,25 177:4,	flat 31:18,21	89:7 91:2,17 92:8
14 85:10	146:12 149:25	9 179:4,5,6,14,20	32:19	93:6 94:7 95:7
extent 9:25	165:2,3,9,10,25	180:7 181:3	flip 20:18	96:2,16 98:1
external 151:2	167:17,21,25	file-specific 71:3	folder 46:17 51:1	106:3 111:17
152:3	168:11 169:11	files 16:20 34:14	60:9,10,24 64:2,4	114:1,15 115:7
extra 81:18	181:13	38:4,19 39:23	65:3,4,5,7,10,24	116:23 120:7
extract 61:5	figured 122:7	40:3,4,10 44:22	66:2,9,15 67:5,6,	123:10,21 124:14
89:16 137:9 180:5	figures 119:21	46:14 47:21 51:8,	10,25 68:1,7	125:24 127:25
extracted 60:16	146:1,13 148:22	17 53:20 55:12	69:14,18 70:5,6	128:16 131:5,22
181:4	165:5	58:7,10,14 59:1,4,	71:17 72:6,25	132:3,12,18
extracting 66:5	file 19:25 20:3	15,22 60:4 61:18	74:1,3 129:25	133:14 136:3
extraction	24:25 26:14 27:17	62:1,9,24 64:13,	folders 58:14	137:14 139:5
106:23	28:20 34:14,17,25	15 65:13,14,25	59:14 64:12,16	140:13 142:19
extracts 68:8	35:2,13,15,16,19,	66:8,19,20,22	65:9,24,25 67:12	145:5,12 146:25
extremely 85:6	24 39:15,16,22	67:17 72:13 73:20	68:5,15	149:19 151:8,16
	40:23,24,25 41:1,	88:25 89:3 95:23	follow 95:18	154:1 157:5 160:7
	40:23,24,25 41:1,	96:13 107:2,15	Foo 35:16,18,19,	161:23 162:24
	6,9,14,15,16,17	116:17,22 119:9	24 38:10,14,19,23	163:22 164:8
	43:3,9,12,14,20	120:13 127:9	fool 102:10	166:6 167:23
	44:4,14,20 45:8,	142:14,17 143:7,	for-profit 86:12	169:24 170:17
	10,14,19,20,21	18 145:19 146:14	force 83:16,25	171:11 172:16
	47:24 51:1,6,13	147:8 150:6	84:3	173:2,25 175:20
	52:8,23,24 53:1,6,	fill 20:25	fool 102:10	176:4 177:18
	7 54:2,3,10,11,15,	filtering 106:25	for-profit 86:12	178:15,22 179:16
	21,23 55:6,7 58:4,	final 12:2	force 83:16,25	180:10 181:11
	19,20 59:8 60:8,	find 47:9,10	84:3	184:23
	13,18,25 61:2,7,	88:16,18 92:2	forever 85:9	format 13:21
	13,15 62:19,21	113:23 114:12,18	forget 88:8	17:8,22 96:9
	63:3,5,12 65:4	118:9,24 120:24	100:12	173:7
	66:2,3,4,5,6,16	121:24 122:17	forgiving 27:16	formatting 13:21
	67:2,5,21,23,25	134:6 135:1	forgot 100:17	formed 14:1 19:2
	68:2,4,6,9,10,14,	143:11 154:25	form 13:3,17	forming 31:18
	24 69:1,3,4,5,6,8,	177:5 184:11,25	15:16 17:18,24	found 27:6,17
	11,13,18,22 70:3,	185:3	18:7 19:4,18	28:20 60:8 61:14
	5,7,18,24 71:7,9,	finds 71:19	20:11 21:9,15	62:20 65:4 68:24
	16,21,22 72:5,7,	fine 9:5,7 44:8	26:1,23 27:4,12,	69:11 89:22
	13 73:12,16,17,25	93:12 104:4	23 29:2,8,25	176:16 178:7
	74:8,16,20 79:21	147:24	30:10,14 31:5	foundation
	80:13 90:1 91:13	fingerprint 91:7	32:9 33:16 40:12	28:10,11
	92:6 95:4,6,22,24	finish 132:13	41:3,11,19 43:15	fragment 154:19
	96:8,13,14 97:12	finished 44:11	44:23 45:23 48:3	frame 108:15
	106:21 107:13,25	167:14	50:13 51:24 52:12	framework
	108:2,13,14		53:9 55:1 57:22	171:18 172:1,6
	115:17,22 117:22,			
	25 118:2,11,13,			
	24,25 119:6,13,			
F				
F-O-O 35:19				
face 91:7				
Facebook 23:24				
24:20 105:15				
Facebook.com				
24:2				
Facebook.com/				
2008 25:7				
fact 31:17 49:15				
83:18 101:2				
fake 91:8				
fall 33:13				
familiar 17:11				
28:25 29:4 109:18				
111:15 123:8,19				
131:20,24 145:4				
family 75:20				

friendly 60:17	Gmail 83:3,23	guided 161:14 164:20 168:7,16 170:4,25 171:13 172:20,24 173:3, 14,19	54:9 55:5 59:9 63:2 67:17 69:12 70:17,22 71:2,8 74:6,7 80:6,12 81:24 83:18 88:16,17 89:21,24 90:16 102:4 107:14 113:9 116:3 117:12,25 118:13,21 123:2 125:10 137:3 143:11 169:4,16 172:1	house 92:1
front 5:24 109:7	goal 87:8 105:6 152:13	guides 168:17	hide 91:25	HTML 30:21
FTP 19:17	good 5:13,14 22:16 56:17 94:12 162:5	guys 83:21 112:18	hierarchy 23:23	HTTP 19:17,23,24 20:5,10
fulfill 105:8 172:4	Google 19:7 20:19 83:1,4,6,7, 17,24 84:4 86:10 105:14 131:20 132:4,11,16 133:1 146:5,6	H	high-level 15:9 24:25 25:18	HTTP:// GOOGLE.COM 17:17
full 5:15 34:18 118:21 122:13	Google's 83:9,11 135:11	hack 87:20	history 131:7	HTTPS 19:23 27:14 83:1
fully 34:5 35:3 36:2,6,10 37:9,12, 16 38:3,4,5 156:8 158:5,23	governed 143:20	hacked 87:11	hold 14:8 26:21 27:11 119:12 120:21 152:12 159:10 169:23 181:21	huge 102:1
function 90:21 105:9 141:13 143:3 145:11 162:4	government 86:16,19	hacker 77:10,13	home 20:2 36:11 82:23 181:4,7	I
functions 34:1 147:14	government-agent 87:18	hair 78:14	home/wei 35:17	i.e. 37:12
G	grad 133:11	half 22:22 104:3 155:5 176:20	home/wei/ documents/foo 36:5	icloud 93:14,15, 17,19
gave 35:11 104:2 105:1 180:25 181:2	graduate 132:23 133:12	hand 20:18 80:17 82:12 88:12 94:2 152:4 163:9	home/wenke 37:20 38:8	ID 117:24,25 119:3,15 120:4,18 122:4,14,17 135:4 176:14,23 177:17, 25 178:5,7,14 179:4,10,11 180:7
general 65:12 93:23 101:17 106:6,12 112:15 128:23 130:10 153:5	grandma 19:12	handed 156:7 158:4	home/wenke/ documents 34:23 36:24 52:9 53:2 55:23	ID(S) 129:15
generally 44:25 74:17 104:24 114:8	grandmom 19:11	handles 122:19	home/wenke/ documents/ filename 35:4	idea 79:7,10 90:22,24 92:10, 22,25 93:3 94:12, 13 128:3 131:1
generate 112:19 117:3,6 138:2	graph 14:25	happen 77:22 174:2 183:7	home/wenke/ documents/foo 36:4 37:13	ideal 76:18 79:16
generated 153:23 155:12,15	graphical 16:6	happened 135:18	home/wenke/ documents/ filename 35:4	ideally 87:5 89:9 183:10
generates 111:3	great 91:22	happening 94:20	home/wenke/ documents/ filename 35:4	ideas 16:4 131:15,17
generating 126:15 155:19	Greek 78:11,25 79:2	hard 36:16 78:21, 23 88:25 92:7 93:2 165:2	home/wenke/ documents/ filename 35:4	identical 48:23 49:17
Georgia 5:19	grow 78:14	head 78:13 96:18	home/wenke/ documents/ filename 35:4	identification 6:7 42:16 109:14 110:3 174:18
gigantic 127:9	GSI 176:13	header 95:10,12, 15,25 96:9,19 98:8	home/wenke/ documents/ filename 35:4	identified 23:16, 21 24:2,3 26:5,10 34:18 39:9,17 40:10,18,23 41:7 121:18
give 12:11,23 16:4 21:24 52:1 53:16 62:4 142:14 157:11 173:24 180:2	guarantee 58:10 86:17,19 87:1 90:23 123:22	headers 95:23	home/wenke/ documents/ filename 35:4	identifier 34:3 38:18 39:3 120:4, 10 179:8,9,14
giving 54:20 77:3	guaranteed 87:5	heading 95:10	home/wenke/ documents/ filename 35:4	
	guess 7:18 9:4 19:8 20:22 30:16 45:17 57:14 63:23 90:4 99:7 138:20 160:10 172:14	heard 12:13 13:1 41:9	home/wenke/ documents/ filename 35:4	
	guessing 31:1 77:5	hearing 28:7,23	home/wenke/ documents/ filename 35:4	
		hey 15:1,22 16:1 21:20 24:24 25:13 37:25 39:13 43:19	hours 10:18,19	

identifiers 34:1 121:15,20 122:25 125:3,14,18 140:10 141:12 142:16 179:1 identifies 57:6 identify 119:16 120:12 121:23 122:15 identifying 34:12 IDS 121:14 124:22 128:25 136:22 141:5 illustrating 23:1 image 26:13 imagine 24:24 99:2 134:10 158:24 immediately 33:3 implement 80:18 82:21 96:7 173:6 implementation 17:9 97:8 117:21 118:22 128:8 184:9 implemented 95:18 implicated 10:1 implies 138:20 imply 50:23 53:19 important 113:22 116:2 160:24 164:9 178:13 importantly 159:1 improve 97:8 incidental 126:6 include 16:10,14, 15 20:9 37:24 38:5,6 51:22 54:5 64:12 65:23,25 71:6 99:6 116:1 119:2,3 121:3 123:16 136:1	137:17 154:19 177:9,20 179:19 includes 34:6,19 37:10,17 43:9 111:9 115:10 123:3 124:7,16 127:19 160:5 179:14 180:7 181:7 including 53:17 incorporate 185:22 incorrect 102:11 increment 126:17 independent 136:14,18 index 111:9,16, 18,22,25 112:2,8, 12,14,15,16,19, 21,23 113:7,11, 17,18 114:2,6,10, 12,17 115:3,10,20 116:7,14,19,20 117:4,7,9,11 119:8 121:3,7,19 122:23,24 123:3 124:7,12,16,20,25 125:7,8,12,13 126:18 127:9,12, 17,19,23 128:3, 18,21 129:5,13 130:8,14,24 131:2,8,9 133:22, 23 134:2,16,18,24 135:5,7,12,14,16 136:18,21,24 137:5,10,16,20 138:16,17 139:3 140:5,23 141:5 142:16 143:2,10, 24 146:17 147:11 148:1 155:16 157:2 177:9,14,20 178:12,20 179:19, 23 180:5,21 181:5,6,18 indexes 111:4 121:9 125:17 126:14,16 134:5,6 138:1,3,5 140:9,	10,25 153:23,25 155:13,15,19 157:22 158:4 178:25 indexing 113:1 indices 156:7,18 158:8,14,21 159:3 individually 182:4,9 184:7 industry 95:19 98:14 inefficient 85:6 information 43:4,9,19 46:9 80:21 87:12 93:24 96:19 98:9 99:6 120:15 134:7 177:9,20 179:19, 23 180:17,22 182:24 infrastructure 86:14 inherit 53:6,15 54:2,24 55:4 56:5 inheritance 50:22 51:11 inheriting 51:16, 17 initial 97:2 initially 142:9 144:7 initiate 144:17 input 140:23 155:12 inputted 155:13 inside 165:12 insist 172:6,7 Intel 97:15 intended 105:8 interacts 165:19 intercept 81:13 internal 75:21 interpret 74:9	108:21 170:3 interpretation 65:1 interrupt 7:17 interrupting 130:5 interruption 81:5 163:3 involved 144:22 ios 89:17,18 90:4, 14 IPR 7:20 8:18 IPR2023-00030 6:11 7:6 IPR2023-0030 6:25 IPR2023-00458 6:4 7:6 9:16,20 22:14 ISP 81:8 J job 31:11 67:13 joke 78:17 junk 92:1 K keeping 90:6 105:1 key 70:13,19 71:3 74:11,20,22,23,25 75:1,5,6,10,11,22, 23,24 76:3,8,10, 12,15,19,21,25 77:3,5,6,7,15,20, 21 79:9,10,12,15, 16 80:2,4,11,13, 14,15,16,20,21, 22,24 81:2,14,21, 22 82:3,8,11,13, 17 83:4,8,9,11,18 84:4,10,11,17,20, 24 85:2,6,7,11,14, 16,17,18,19,22	86:3,4,8,9,10,14, 18 88:1,2,3,4,7,8, 13,15,17 89:2,3, 13,21,25 90:11, 13,16,18,24 91:1, 13,15 92:6,10,16, 17,18,23 93:1,4 94:5 95:20 101:23,25 102:2, 4,5,10,11,16,19, 21,23,24,25 103:2,3,6,7,8,12, 13,15,19 104:6,8, 11,14,15,19,24 105:2,5,7,9,13,16 151:22 155:11 157:11 159:6 169:22 182:6,11, 12 183:2,11,23,24 184:2 key-pair 95:1 key-private 86:18 102:25 103:7 Keychain 89:18 90:5,7,8,14,22,24 91:16,20 93:4,13, 14,16 keys 74:23 82:17 86:24,25 89:16, 19,20 90:6 94:24 101:10 103:19 105:1 158:24 182:15,18 183:15 keyword 113:10 114:18 115:5,20, 21 116:20 117:9, 10 125:1,2,11,12 130:23 133:2 134:2,11 143:19 180:1 183:2 keyword-based 127:7 134:12 keywords 111:10,12,22,24 112:7 113:2,4,14, 20 115:4,11,13,15 116:2,4,6,8,10 117:13 121:4,6 122:25 123:4,6 124:8,10,12,17, 19,21,22 127:20,
---	--	---	--	--

22 128:4,6,25 129:14,18 130:16 134:14,22 135:1,3 136:22,23 137:3, 10 155:12 177:15 178:25 182:15,18 kill 85:8 kind 14:17 15:2 22:7 44:25 64:15 74:24 78:14 80:23 81:14 86:24 88:11 90:20,21 91:9 94:16 95:19 96:8, 10,18 97:9,19 98:9,15,20 101:17 103:11 106:6 108:1,8 128:4 130:23 131:2,14 133:7,23 134:7,22 137:21 150:2 160:24 164:1 166:20 167:5 169:23 174:6 176:19 179:8 182:22 184:2 kinds 75:3 94:7 108:10 knew 88:19 146:20,21 knowing 77:20 79:16 80:15 82:5 knowledge 12:24 31:1 102:12 L L-E-E 5:17 language 30:21 42:2 123:15 173:7 laptop 79:20 Larry 132:9 law 83:21,22 laying 93:25 leaf 44:21 leak 182:24 183:9,10 leaking 183:8	learn 156:20 157:18 158:16 159:7 leave 93:25 lecture 82:24 Lee 5:2,6,13,17 9:25 11:10 12:10 28:14,24 56:14,21 86:10 109:6 110:21 114:10 149:8 186:10 left 132:8 135:18 165:11 left-hand 24:16, 25 25:15 141:25 legal 17:22 18:1 letters 82:2 libraries 123:16 lie 85:23 likewise 162:14 limited 7:24 28:5 link 142:5 linking 15:6 list 24:25 25:3,15 113:20,21,22 128:4,5,20,24 listed 101:3 literal 30:22 load 7:13 147:10 loaded 123:12 134:6,16 147:9,10 160:9 local 20:1 34:4 35:8 38:10,13,24, 25 39:2 40:5,11 41:1 141:12 locate 112:6 118:1,24 119:5 120:10 134:13 located 5:18 146:21 locater 17:15 26:11	location 155:10 locations 119:9 log 93:21 94:18 107:14 long 10:17 22:2, 10 34:19 35:3 56:9,12 81:23 83:10 93:5 98:20 104:2 110:15,19 128:14 130:11 131:7 148:16 longer 57:13 153:13 looked 22:10 131:7 lose 88:3,7,18 89:3 losing 90:11 lost 46:4 88:7 89:22,25 108:2,14 129:21 lot 82:23 84:8 87:1 94:9,11,13 105:11 120:1 lower 165:10 LU 5:12 6:8 7:22 8:19,24 9:4,14 10:7 13:12 14:5 16:8 17:21 18:3, 23 19:14 20:8 21:3,10 22:4 26:15 27:1,7,18, 24 28:3,12,13 29:5,11 30:1,5,12, 17 31:14 32:16 33:22 40:2,21 41:8,13 42:5,17 43:21 45:6 46:11 48:20 50:18 52:5, 21 53:10 55:17 56:10,13,20 58:5 59:11 60:1 61:8 62:12 63:11,20 64:24 67:3 68:22 69:24 71:5 72:3 74:10 76:1 78:1, 24 79:19 82:6 83:12 87:24 89:8 91:11 92:4,21 94:21 95:21 96:11	97:10 98:5 99:10 100:7 108:24 109:10,15,25 110:4 114:5 115:2,16 117:17 120:8 123:13 124:2,24 127:11 128:11 129:19 131:18 132:1,7, 13,15 133:10,15 136:17 137:19 139:8 141:8 144:1 145:7,15 147:17 148:17 149:2,7,22 151:12 152:9 154:5 157:13 160:17 162:10 163:13 164:11 166:10 168:4 171:6 172:9,23 173:12 174:7,15, 20 175:21 176:5 177:22 178:18,24 179:24 181:8,16 185:9,23 186:5 luncheon 99:14 lying 85:23 86:2 M Mac 89:17 90:4, 14 91:15,20 93:4, 11 machine 20:3 88:9,11 made 126:6 magically 46:25 main 105:22 maintain 119:22 maintained 120:15 152:5 maintaining 151:1 152:2 make 45:4 47:25 53:5 54:23 70:23 80:8 94:8 97:4 100:13 101:18 103:17 105:7 108:21 147:12	148:20 149:25 153:6 167:7 173:13,16 174:2 makes 147:7 making 161:20 malware 106:25 man 81:4,7,8,11 83:19 87:15 102:8,9 manage 163:7 managed 13:11 management 58:13 59:13,20 60:3,15,23 61:2 67:13,21 68:5 69:3 74:2 103:15 106:22 149:23 150:5 160:13 manager 89:14 manages 167:21 170:15 manipulated 161:8 manner 19:3 manual 80:7 map 122:23 123:2,9,12,18,23, 25 124:4 mapped 129:14 176:13 mapping 122:25 marked 6:7 42:16 109:14 110:3 174:18 master 89:15 match 113:12 matches 156:19 158:15 mathematically 78:22 matter 12:7 47:9 122:5 137:12 184:21
---	--	---	--	---

meaning 13:9 16:24 20:4,24 25:12 26:7,8 31:11 33:3 34:12, 19 36:3 39:3 40:14 46:4 47:6,9 48:6,9 51:16 67:23 69:13 75:23 77:5 78:18 79:18 81:7 86:8,23 88:7 90:15 94:8 95:13 97:3 101:25 102:20 105:6 107:11,22 114:21 115:24 116:11 119:15 120:18 127:16 134:25 143:16 144:16,17 148:6 152:3,15 160:21,23 162:6 163:5,6 168:16 169:6 174:5 185:11 means 13:7 23:19,23 25:5 26:3 30:13,15,22 36:15 37:4 49:7, 16 61:16 62:7,22 92:17 107:24 111:25 113:13 118:6 122:11 137:22 146:4 157:1,7 162:16 163:9 168:15,23 169:20 172:25 meant 14:8 101:19 measure 49:9,16 measuring 49:10 mechanism 77:1,18,24 126:20 135:8,9,22 136:6, 9 137:12,21 138:2,4,6,8,10,14, 18,23,24 139:2,4, 14,15 169:21 181:10 183:16 mechanisms 76:8 97:12 113:8 117:3 126:17,18 136:2 172:19	meet 10:8,15,17 member 163:10 memory 94:4,6 123:25 141:12 mention 114:23 183:19 mentioned 97:13 113:16 met 48:7,8,12 metadata 43:1 51:1,13,14 60:16 61:6 66:18 68:8 156:21 157:19 158:17 method 59:8 60:17 65:22 70:19 71:4 75:10,19 77:18 90:8 181:20 182:1 methods 101:10 117:6 141:17 Microsoft 86:22 middle 65:21 81:4,7,9,11 83:19 87:15 102:8,10 119:22 122:8 156:6 176:19 Mika 22:24 million 24:8,13 25:8,23 minus 31:23 32:4,23 33:10 minutes 56:16 missing 21:1 misunderstood 37:7 44:9 model 12:20 14:13 16:23 65:18 modern 79:7 82:15 modern-day 78:20 modified 41:16 modify 41:15	moment 15:13 148:21 monitor 59:21 67:9,21 71:18 74:2,3 94:16 147:12 monitoring 67:9 monitors 58:13 59:14 72:6 147:13 morning 5:13,14 move 7:18,21 8:9 88:9 99:10 145:23 174:9 moved 43:4 movie 85:8,15 moving 33:23 multiple 23:24 45:8 58:3 65:2 74:22 77:9 94:23, 25 95:2 101:21 108:10,12,18,19 120:17 146:1,7 148:2 152:15 171:22 music 39:23 40:4,9,10,16 N names 13:10,13, 15,21,25 16:11 17:6,8 31:19 32:2 33:18 38:1,5,13 52:17 namespace 23:2,10,12,14,16, 17 24:4,9,19,21, 22 25:3,6,17 26:3, 5,8 28:17 30:8 31:21 32:2,7,19 33:5,9,14,24 34:4, 7,11,13,25 35:9, 12,23,24 37:1,3, 18,21,23 38:11, 14,17,21,22 39:4, 7,9,14,15,20,23 40:9,14,17,19 118:17,19,20 121:24 122:16	namespace's 34:12 namespaces 22:25 31:17 39:21 namespece 37:3 naming 13:2,5,9, 16,20,24 14:11,17 32:12 120:13,14 nearby 52:16 53:22 necessarily 113:17 negotiate 80:20, 21 81:14 83:8 98:25 negotiated 80:5, 12 negotiations 99:4 nice 148:8 node 44:19 nodes 44:21 nonencrypted 66:1,8 normal 95:23 128:7 Notably 121:17 Note 46:14 notes 5:23 noticed 100:15 ns# 25:24 nuance 70:10 number 6:6 10:19 25:5 31:22 32:3,14,20 33:3,4, 6,9 42:15 80:6,7 81:25 94:1 101:8, 9 109:13 110:2 113:23 174:17 175:1 numbers 33:18	O oath 9:1 object 23:13,16 26:10,11,12 39:8 40:22 object-oriented 16:6 objection 13:3, 17 15:16 17:18,24 18:7 19:4,18 20:11 21:9,15 26:1,23 27:4,12, 23,25 28:11 29:2, 8,25 30:10,14 31:5 32:9 33:16 39:25 40:12 41:3, 11,19 43:15 44:23 45:23 48:3 50:13 51:24 52:12 53:9 55:1 57:22 58:22 59:17 61:4 62:3, 15 63:15 64:5 66:10 68:11 69:9 70:9 71:14 72:10 75:16 77:16 78:7 79:13 80:3 82:19 87:13 89:7 91:2, 17 92:8 93:6 95:7 96:2,16 98:1 102:5 106:3 111:17 114:1,15 115:7 116:23 120:7 123:10,21 124:14 125:24 127:25 128:16 131:5,22 132:3,18 133:14 136:3 137:14 139:5 140:13 142:19 145:5,12 146:25 149:19 151:8,16 154:1 157:5 160:7 161:23 162:24 163:22 166:6 167:23 170:17 171:11 172:16 173:2,25 175:20 176:4 177:18 178:15,22 179:16 180:10 181:11 184:23
---	--	--	--	--

objects 26:9 34:11 39:5 obtain 82:17 91:1 175:12,19 182:6, 8,12 obtaining 175:16 obtains 140:25 143:1 obvious 53:25 94:1 97:6 121:12 officer 160:12 offset 176:24 177:1,5,10,16,21, 24 178:9,10 179:6,15,20,25 180:8 ogp.me/ns# 24:14 ogp.me/ns#. 24:7 old-fashioned 82:10 operation 106:20 operations 15:5 operator 156:13 opinion 31:3 101:24 optional 18:14 21:1 order 106:19 114:9,24 146:20 152:16 ordinary 107:10, 22 127:15 135:11 organization 15:3 22:6 47:1,2 83:16 98:18 organizations 83:16 organize 15:4 16:19 40:15 41:5 organized 13:8 14:13 15:1 16:5 114:24	original 41:15 43:13 45:20 47:24 53:7 61:16,24 62:7,22 63:5 69:7 71:25 79:18 133:5 182:16 orthogonal 137:1 138:17 185:7 OS 90:14 91:15, 20 93:4,11 outsider 97:6 overloaded 65:2 111:19 overly 112:24 owner 158:9 owner's 10:22 owns 48:15 143:13 P p.m. 99:15 109:3, 4 149:5,6 186:7,8, 13 Pacific 5:1 pages 129:16,17 175:11 176:8 180:23 181:3 182:4,5,7,8 184:3, 6,16,17 185:7,11, 12 pair 84:11 86:18 102:25 103:7,8 pairs 75:6 paper 82:11 91:24 132:9 133:6 papers 131:16 paragraph 22:15,16,17,22,23 23:11 31:17 37:8 38:16 42:18,20 43:2,18,23 44:1,3 45:15 46:14 48:5 52:1 57:6,10,14 58:1,6 60:7 63:18 65:21 73:18	100:21,24 106:16 110:18,20 111:2 113:6 117:1 120:25 121:11,13 126:1,9,11 127:8 129:9 135:18 137:23 139:12,19 140:3,7 142:22 143:6,22 150:4, 10,13 153:14 154:7,16 155:1,2, 3,21,22 156:12 159:10,18,22 161:20 164:17 165:3,24 166:8,9, 23 167:2,5,20 170:21 172:18 175:3,8 176:7,11 177:7,23 179:18 181:2,22 paragraphs 22:19 49:24 174:23 177:3 parameters 98:9 pardon 105:24 parent 34:20 38:7 41:16 43:14 44:20 45:8,20 54:3 61:17,24 62:7,23 63:5 69:7 71:25 72:23 parent/child 53:21 part 12:5 28:4 31:11 37:13 57:24 71:9 95:9 105:5,6, 10 117:1 118:2 175:10 182:7 pass 8:12,25 9:10 185:24 passage 44:13 passing 8:3 password 89:14, 16,19 91:5,7,21 92:17,19 93:5,11, 14,15,19,20,21 patent 6:12,13,14 7:1,7 8:7,9 10:22 42:1 48:5 49:21 53:14,25 55:3	59:19,24 67:16 68:16 70:11,14 72:15 73:5,6 74:9, 13,15 100:17,25 101:2,13 102:4 106:9 111:20 112:25 117:15 128:10,15 129:8,9 131:13 132:21 141:20 144:20 145:1,2 152:7 155:4,21 163:24 164:9,10 165:5 185:8 patent's 70:22 patents 10:23 41:22 path 118:21 120:19 122:13 payload 154:18 PDF 29:18 57:11 106:16 110:19 139:20 150:11 153:15 159:11 174:22,25 176:8 people 16:4 20:6, 15 77:6 80:6 86:12 102:3 103:3 105:12,19 108:12, 19,21 114:25 116:6 128:17 130:19,21,22 160:13,15 163:7 164:4 183:1 percent 90:23 percentage 11:19 perfectly 19:11 perform 141:4 145:18 148:9 154:22 155:7 performed 58:3 performs 147:14 148:24,25 149:24 151:7,15,18 period 60:14 61:1 66:4 68:8 permission 74:5	143:8 permissions 52:3 73:21 person 84:15 88:14,21 90:25 127:15 personal 101:24 personally 17:2 petition 9:20 phone 82:4 photo 51:14 photos 59:21 physical 109:7 piece 40:18 82:11 91:24 93:24 118:1 pile 91:25 PKI 95:19 place 36:17 46:25 52:17 54:15 73:20 88:9 89:15,18,22 107:11,14 144:23 147:13 148:7 154:4,6 placement 50:11,16 51:6,7, 21,22 52:2,6,7,15, 23 53:6,16,17 54:2,5,10,16,21, 24,25 55:4,6 57:25 72:21 73:7, 15,25 74:1 places 18:17 65:14 89:14 114:13 122:20 plain 92:23 107:10,22 plaintext 79:18 91:13 92:6,10 93:1 plan 7:25 148:16 plenty 21:24 104:3 112:22 127:1 plurality 175:12, 17 180:17 182:3,
--	---	---	---	---

6,8,12 184:17 point 32:11 41:5, 20 42:1 54:14 55:20 66:25 70:20,21,22 73:22 74:13 80:23 81:13 97:5 101:13 102:15 103:5 106:9,13 114:6 116:5 119:5 122:6,12 144:14 154:6 173:8 185:4 pointer 113:12 115:5,21 117:18, 22,23,25 118:5,7, 12,20,23 119:15 120:3 pointers 111:11, 23 113:3 115:12 116:9,21 121:5, 13,22 122:2 123:5 124:9,13,18,21 127:21 128:25 135:4 136:22 pointers/ identifiers 121:17 pointing 26:11 165:13 points 105:22 policies 50:16,20 51:18 52:2 53:17 57:7,20 72:21 74:1 164:2 171:17 172:6,25 policy 50:11,24 51:6,7,11,22 52:7, 23 53:7,16 54:2,5, 10,16,21,24,25 55:4,5,6,11,14,19, 20,23 57:25 61:15,17,23,24 62:5,8,11,13,16, 21,23 63:2,3,10 68:25 69:4,21 70:8,21 71:20,23 73:9,15 74:6 143:21 159:20,24 160:2,14,15,22,25 161:2,5,15 163:18,20,25	164:5,6,7,22 165:13 166:1 167:22 168:2,8, 12,17,19 169:4,6, 17,19 170:12,13, 14 171:1,8,10,14, 17,18,20,24,25 172:1,4,6,8,12,21 173:1,6,8,18,20, 22 popular 97:15 portion 50:10 57:19 POSITA 70:15 71:1 73:23 74:9 97:6 102:12 103:6 121:13,21 169:2 171:16 181:17 184:20 POSITA's 70:20 position 82:2 possibles 70:20 possibly 117:23 power 87:22 practice 162:5 practiced 130:18 131:1 precaution 103:9 precise 14:2,4 precisely 42:3 precomputer 78:4 predetermined 66:3 68:8 prefix 29:13 preliminary 10:22 prepare 9:22 10:6,9 presume 100:24 pretend 83:24 pretty 7:24 66:16 78:21,23 98:17 110:19 114:9	143:23 144:2 147:5 148:23 178:20 previously 6:6 42:15 109:13 110:2 167:10 174:17 principal 81:12 printed 5:25 42:8 printout 27:2 prior 109:7 126:25 131:13 132:5 147:20 priority 100:16, 24 101:3 131:12 private 84:20 85:1,2,17 92:18 102:25 103:6,7,13 104:8 105:2 privileged 10:1 problem 76:20 80:10 102:6 104:12,14 problems 87:2 proceeding 8:11, 18,22 9:12 proceedings 8:6,15 186:13 process 12:5 processing 66:4 182:1 processors 110:16 produce 121:8 product 10:1 products 98:16 program 34:2 programming 123:15 programs 94:8, 10 promised 104:17 pronounce	109:12 proper 12:11 106:5 122:19 protect 92:19 161:15 164:22 166:17 168:8,25 171:1 protected 83:9 152:24 171:4 protection 171:22 174:4 protects 171:8 protocol 19:16, 24 20:10 provide 20:16,17 33:25 38:17 39:12 63:25 112:13 126:9 135:9,23 136:7 152:14,16 153:2 provided 59:1,5 66:23 provider 122:11, 21 147:2,11 148:11 156:13 providers 111:7 141:16,19 146:2, 4,7 148:4 152:1 providing 131:13 proxy 83:22 85:23 86:2 87:16, 21 102:8,9,14 152:20 public 75:1 83:4, 9,11,15,17 84:4, 10,17,24 85:6,7, 10,19,22 86:8,14, 18,24,25 95:20 101:23,25 102:2, 5,11,19,24 103:2, 3,7,19 104:6,7,11, 12,13,15,19,24,25 105:5,7,9,13,16 public-private 75:5,6 95:1 publicize 105:16	published 98:19 133:6 pull 26:17 175:24 purely 59:7 purpose 39:6 112:2 131:11 147:4 purposes 148:3 put 9:1 15:3,15 19:20,23 20:13 21:16 27:19 31:15 38:6 47:5,17 55:7, 10 56:3 67:10 78:13 89:15 90:9, 13 92:10,15,19 93:1,12 95:10 97:3,16 102:21 103:10 104:15 107:11,25 108:23 137:10 140:20 143:21,24 144:21, 22 147:5 148:3,6 152:10 153:8 174:2 185:8 putting 18:24 55:22 73:22 104:21,23 122:19 148:2 157:16 Q qualified 34:5,19 35:3 36:3,6,10 37:9,12,17 38:3,4, 5 qualify 22:1 42:2 queries 156:17, 22 157:20 158:13, 17 query 140:4,8,11, 23 142:25 158:11 159:1,3 question 11:14 21:11 30:2 37:7 40:6 41:25 44:9 56:7 66:20 107:6 124:11 132:14 145:14 151:11 155:18 167:14
---	--	--	--	---

178:17 184:9 186:10 questioning 7:23 8:9 questions 7:5,24 8:16,18 9:9,19 185:24 Quincy 7:16 80:14 81:24 88:17 quote 43:3 68:24 164:19 167:5 quote/unquote 21:1 quotes 81:16	ready 100:8 real 84:5 113:18 reask 122:23 140:6 151:13 reason 6:21 47:1, 14 85:5 87:17 108:2 139:17 151:10 reasons 87:15 151:14 recall 7:2 10:19 17:14 133:22 181:15 receive 145:19 receives 142:24 recess 56:18 99:14 109:3 149:5 186:7 recited 122:7 recollection 132:23 recommend 85:5 92:5 93:20 record 5:16 8:15, 22 9:8 28:2,3 35:20 36:15 81:6 100:11 107:12 126:7 163:4 records 153:22 180:16 recover 89:4 redundancy 54:13 refer 35:8 36:22 37:8 39:19 65:3, 13 75:21 101:9 reference 52:10 57:1 110:1,5,12, 16 129:8 130:24 131:3,16 154:13 155:2 157:8 164:7 references 109:21 referred 34:3 65:7 75:22	referring 15:11 18:19 42:7 63:17 64:18 refers 24:16 63:12 reflect 104:3 regular 94:18 regulated 17:23 18:6 regulates 166:3 related 46:17 55:12 relational 14:24 15:1 16:5 relationship 16:25 45:1 53:21 167:18 released 132:2 relevancy 28:8 relevant 47:18 70:16 132:20 133:19 134:7 rely 109:22 110:13 remained 66:3 remember 12:8,9 29:3 41:21 73:6 81:1 89:23 102:17 133:4,5 147:15 150:2 Remote 5:2 remove 68:2 90:1 103:3 removes 175:10 182:7 repeat 40:6,8 145:13 151:11 178:16 rephrase 92:24 report 109:22 reporter 22:13 81:5 163:3 repositories 46:16 47:2	repository 46:3, 13 47:8 48:19 54:12 request 144:21 169:24 requests 94:16 require 17:7 19:15 48:17,18 137:20 required 18:14 21:21 requirements 108:23 requires 61:25 71:9 research 24:11 resembles 31:4 reserved 7:19 resource 17:15 respect 21:7 105:2 107:6 181:18 respond 140:6 responding 140:5 response 10:22 responsibility 160:22 responsible 160:25 162:11 rest 68:16 restart 9:11 restarting 8:4 restricted 53:1 restricting 54:21 restriction 54:6 result 96:24 97:4 156:6 158:3 183:7 results 156:22 157:20 158:18 retained 12:6	retrieve 89:20 108:4 122:21 145:10 146:22 retrieved 142:3 161:8 retrieves 140:9 141:14 return 125:14 156:18 158:14 returned 141:13 returning 159:4 returns 125:17 140:10 142:2 review 10:20 22:18 reviewed 10:21 reviews 22:20 44:10 50:8 57:17 64:7,20 107:4 110:24 126:3 140:1 150:16 153:19 154:14 156:4 159:16 167:12 175:5 176:9 revised 11:22 right-hand 25:4 26:4,7 49:21 rocket 99:8 role 160:14 Roman 79:3 Romans 78:12 79:1 room 5:20 root 36:7,16 44:19 45:14 51:19 55:5,6,11 rooted 45:9 50:25 51:12 Roughly 29:23 round 99:4 router 79:24,25 80:11,15,25 81:8, 10,11,19,20 82:4,
R				
random 94:18 97:3 range 31:22 32:13,21,23 33:10 112:4 rank 133:3,23 rarely 77:22,23 RDF 30:7,8 read 21:17 25:19 31:24 43:25 44:5, 7 46:19 50:3 51:3 53:14 54:17 57:14 58:16,24 62:17 66:12 67:15 68:15 73:6 83:2,7,23 109:20 110:20,25 111:13 121:1 131:19 132:9 133:5,20 136:20 138:22 139:22,23, 24,25 143:13 150:2,13 151:4 153:17 155:3 156:3 157:23 158:2,19 159:13 161:18 181:22 reading 20:14 21:4 41:21 44:11 65:22 98:13 133:4 141:20 167:14 170:20				

7,12,17,21 83:2 86:2 87:6,9,14,16 row 24:6 26:19 Rule 80:6,7 94:1 rules 50:23 51:11 S S215 175:9 S220 180:14 S225 180:14 save 106:19 Sb 49:4 scenario 60:7 61:10 62:5 67:7 68:13,18,19 71:7 108:9 scenarios 60:3,6 68:14,17 schema 12:10, 12,14,16,17,18, 19,22,25 13:1,6,8, 9,24,25 14:3,7,10, 12,22,23 15:8,14, 20,24,25 16:10, 14,16,23 17:6,23 18:6,9,16,18,21 30:7 31:2,4,6,8,9, 12 33:20 schema's 31:11 scheme 85:10 86:21 87:2 schemes 95:9 school 132:24 133:12 science 99:8 106:6,13 118:6 scope 13:15 14:2,4 33:25 34:7, 11,13,21 36:22,23 37:2,4,10,14,15, 18,24,25 38:1,4, 18 39:5 40:19 47:4 106:5 screwed 91:9	scroll 165:2 search 19:7 112:4 113:9,10,14 114:18 116:4,6,8 121:19 125:6,11, 16,17,21 130:16, 22,23 131:20 132:4,11,16 133:2,9,21 134:11,23 135:6, 12 140:17 141:4 143:5,7,17 144:18 145:11,18 146:8, 19,24 148:9 154:20,21,24 182:21 searchable 113:8 117:2,5 121:7 126:14,17, 18,23 127:2,5 128:3 130:8,10,20 131:6 135:8 137:6 138:1,3,5,9,10,14, 22 139:4,15,16 140:18,21 143:10, 24 150:25 152:1 154:23 searched 129:17 141:6 161:9 searching 132:24 143:9 144:24 secret 91:5 93:24 103:6 section 63:23 sections 23:3 secure 64:12,17 65:10 72:25 74:3 90:6,7 91:4,15 92:3 102:23 103:9,15 104:7 105:2,8 secured 65:23 66:2,9 67:5 68:1, 5,6 70:6 90:25 104:9 security 52:19 59:9 90:20 91:6 97:8 105:6 148:3 160:12 162:5	171:21 174:4 sees 60:24 68:6 segment 117:24 119:3,6,17,24 120:14 segments 119:2 selective 158:7 send 47:25 76:10 79:21,22 84:14,24 85:11 88:14,17 98:22 99:6 142:13 sending 140:4 158:10 sense 78:17 99:8 134:15 144:16 151:24,25 184:14 sentence 34:9 106:18 142:23 144:3 156:16 157:18 168:2 175:8 separate 8:14,16, 22 164:21 165:18 184:5 separated 161:14 168:7 170:25 173:20 Sergey 132:10 server 25:2 58:13 59:13,20 60:4,15, 23 61:2 67:13,21 68:6 69:3 71:19 74:2 76:22 94:15, 17,19 106:22 118:18 140:24 141:10 142:2,13, 15,24 143:1 145:18 147:3 149:17,24 150:5, 20,22,25 152:1 163:21 servers 106:21 service 54:13 58:11 71:17 72:6 86:4,5 90:4 156:13 services 106:24	107:1,2,8 session 121:16 set 116:5,8 123:16 129:13 130:15,24 131:3,9 134:18 159:19,23 160:1,14,15,23 164:5 180:18 sets 163:18 166:1,2 setting 160:22 163:19 SFTP 79:22,23 shape 164:8 share 90:15 shared 93:17 158:24 shares 51:23 sharing 52:3 74:5 shave 78:12 Shifka 110:5 111:21 112:25 115:3,18,19 116:19 117:15,18 121:11,14,16 122:22,24 124:7 125:8,20 126:1,5 127:12,13,17 128:9,15,19 130:11 131:15 134:17 135:2,15, 17 137:8 139:19 144:15 145:17 147:6,22 148:21, 23 149:13 150:9 151:6,15 153:6 178:21 179:3,7 Shifka's 121:3 124:25 shift 97:1,2 ship 20:20 shocked 21:25 short 7:23 34:4, 15,16 35:1,8 38:10,13,24 40:4, 11 41:1 108:25	148:15 show 58:15 59:15,22 68:15 71:17 72:5,13 112:20 shows 67:2 72:5 74:14 114:20 side 20:18 24:16, 25 25:4,15 26:4,7 142:1 147:23 sides 80:22 sign 86:4,24 signature 11:7 66:5 signatures 84:1 104:23 significant 129:13 130:15 131:9 134:18 135:11 148:5 175:13,17,24 177:15 178:13 180:16,18,24 181:4,6 182:9,10, 13 sim 49:7 97:18 similar 13:7,24 14:6,8 48:9,10,22 49:12 52:17 53:20 61:13 62:19 69:12 71:16 115:3 131:17 178:20 similarities 44:4 50:17 similarity 48:12 49:1,5,8,16 simple 33:4,5 41:7 75:10 94:1 simply 31:22 32:20,25 single 11:15 31:18 46:15 47:22 76:8,9 88:2 96:22 106:20 108:17 117:6 152:17 172:8 180:20 184:7
---	---	---	--	--

site 20:24	139:16 140:17,19, 21 143:3 146:20 147:2,3 181:14 184:10 185:6	stays 46:7	structures 12:20 123:17,20	suppose 41:14
situation 54:23 69:2 82:13 84:13 94:14	specifically 19:25 63:4 108:22 131:8 134:21 154:10 160:25 166:16 172:2 179:3 185:2	steal 87:12 102:10 103:12	students 89:24	supposed 15:18 79:17 92:18 93:16,24 104:12 143:13 169:16
skill 127:15	specifies 184:1	stealing 76:25	studied 25:18	supposedly 151:19
skull 78:14	spend 98:13	steals 88:25	studying 30:25	sur-reply 6:10
slash 19:25 36:12,15	spent 30:24	stenographic 126:7	stuff 49:13 84:1 89:15 99:8 132:25 134:12	surprise 99:1
slightly 64:23 66:14	SSH 92:13,17	step 72:4 175:9 180:14 185:14	stupid 78:14	surprised 21:19
so-called 79:18 83:17 84:4 86:14 97:18	staff 159:19,23 160:1,5,8,9,10,11 161:21,25 162:1, 13,20,22 163:1,6, 9,11,17 164:4,15 165:25 167:21 168:1 172:11	steps 63:24 68:4	subdirectory 23:4,25 25:8 34:18 35:1,21 38:22,23	survive 54:13
somebody's 20:25	stand 17:13 80:17	stolen 103:1	subject 48:25	sworn 5:7
something- something 25:9, 10	standard 18:20 20:14 21:5 22:6 85:20 95:9,19,20 96:6,20 97:14 98:13,18 123:16 141:16	storage 58:3,7,11 59:5 66:23 88:8 90:19 103:15 106:20,21 107:1,8 108:1 111:7 118:13,18 119:25 120:17 122:11,21 141:15,19 144:22 147:3,11 148:11	submit 8:2 28:16	SWS 129:13
sort 15:5,15 21:13 28:25 29:1 32:3 44:14 63:19 67:16 94:6 140:24 166:17	standardized 21:13	store 15:18,20,23 16:25 76:21 89:13,19 91:20 92:6,10,23 93:1,3 102:16 122:10 155:10,17	submitted 6:4,10 9:20 28:6	Symantec 86:22
source 23:20 26:11	standards 18:11 21:7	stored 16:24 92:20 108:4 111:6 119:18,24 120:14, 16 122:10 141:11 161:6 163:20 164:3,8	subpolicies 172:5	symmetric 76:5, 6 85:16,18 88:1, 13 89:2 94:24 101:23
sources 23:19	stands 17:14 97:13 122:11	storing 91:15 146:6 148:11 163:24	subscribers 158:12	symmetry 74:25 75:20,22 76:3 79:9,15 85:11,14 102:4,18,21,23 103:8,12,19
SP1 122:10,11 146:3	start 14:23 18:12 36:9 50:5 100:9	stretching 53:13	Subsequent 158:6	synchronization 107:2
space 24:7 39:2 86:14	started 101:16	strictly 118:8	subtree 50:25 51:2,13,14,17,19 72:21 73:8	system 39:22 40:24,25 58:3,4 71:8 79:8 82:16 96:13 140:8 145:3 147:12 150:19 162:7,16 163:1,2, 5,6
speaking 118:8	starting 44:3 49:24 154:7	string 19:1 30:22 32:6,14,22 33:13, 19 34:16 122:14	sufficient 118:16	systems 82:16 163:8
spec 143:6	starts 81:15	strong 77:7 78:18 93:5,11 173:15	suggest 19:7,8 20:15,23 33:4 50:15 56:12 64:16	
special 58:15 59:15,22 64:9,15 65:8 67:25	state 5:15 87:18	structure 31:18, 21 32:19 44:18 45:9 46:17 123:9, 23,24 124:4	suggested 68:13	
specialized 133:23	statement 152:7 153:6		suggesting 49:18	
specific 10:2 14:15 15:10,24 16:17 49:2 51:23 52:14 53:18 54:6, 22 61:13 62:19 63:9 68:24 69:21 75:21 127:17 134:19 136:15,19 137:21 138:10	status 65:23 162:17		suitable 108:22	
			super 85:15 91:22	
			supplemental 7:22	
			supplementary 7:10	
			supply 98:15	
			support 15:4	
				T
				T1 141:11 146:9
				T2 146:9
				table 12:20 15:4 16:11,12,20 17:5 23:1,7,18,20 24:5, 6,10,12,15 112:16,19 119:18, 23 122:9,20 128:20 134:24

137:5 141:11 146:9 tabulated 22:24 tag 154:19 tags 154:18,23 takes 85:9 146:6 talk 15:25 21:19 23:22 24:17 25:5 37:1,2,19 39:4 56:22 57:24 59:7 62:17 69:10 70:11 72:11,20 73:6,8 75:9 76:2 77:19 78:10 98:16,20 102:18 103:19,25 106:10 109:23 117:23 118:10 119:1,21 120:21, 22 123:24 126:22 129:9 130:20 132:23 133:2,7,22 134:20 135:3 144:15,19,20 145:1 146:1 147:12,21 149:9 150:8 154:15 163:24 166:8,13, 16,20 182:22,23 183:18 184:4,5, 12,25 talked 90:3 talking 12:16 14:18 23:14 29:17 35:23 36:7,25 37:1 44:13 46:12 50:10 57:20 58:6, 24 63:14 68:3 74:15,25 76:24 83:5 84:10 106:6, 12 135:14 138:15, 16 140:3,7 144:18,24 145:2, 17 165:3 talks 13:25 26:4 41:22 45:3 50:16 53:15,17 60:5 66:21 69:19 70:15 72:12,15 73:5,19 101:3 113:1,7 117:15 119:14 122:8 125:8	126:2,11,13,16 127:17 128:9 129:3,5 131:14,16 134:18 135:15 136:21 146:3,14 147:23 153:7 154:3 155:4,5,19, 21 157:9 164:10 172:1 179:4,6,18 180:13 181:2,13, 24 182:14 183:23 185:16 taught 123:23 185:8 teach 78:9 80:5 teaching 59:20 136:14 185:1,6 technical 16:9 TEHRANCHI 175:20 tells 15:20 43:18 59:12 73:15 95:12 96:9 115:14 119:23 120:13 122:9 123:2 term 12:13 15:9 17:11 18:9,16,18, 21 41:9 43:17 44:16 66:14 74:14 107:8 111:19 112:24 123:12 128:18 134:6,16 140:11 149:20,23 150:1 160:9 termed 45:10 terminology 18:25 terms 21:1 30:7 48:11 65:2 106:1, 10 108:21 118:6 119:24 125:22 184:9 test 141:13 143:3 testified 5:9 136:2 testify 5:7 testifying 82:15	testimony 12:4 21:6,12 25:25 105:1 120:9 text 15:21,23 19:1 81:15 91:13 92:6 93:25 94:6 115:17,22 134:24 135:1,13,14 textbooks 98:16 thing 20:7 49:2 64:18 66:13 78:10 86:7 88:11 89:18 96:10 97:3,9,19 98:10 102:7,20 106:7 108:16 123:24 127:13 132:25 134:11,24 166:3,21 169:23 182:22 things 8:4 13:2,6, 22 14:12 15:10 16:13 17:1,4 20:13 24:23 25:14 31:13 32:13,14,17 48:11 49:12 52:14 59:10,12 73:4,23 75:3 78:4,13,15, 17 81:1 83:6 84:9 93:23 94:7 97:5,7, 17 98:21 100:10 101:18 102:11,14 104:24 107:11 108:8 118:8 120:1 122:19 128:20 147:7 160:24 167:8 172:3 174:6 third-party 86:4, 5 thought 105:23 throat-clearing 105:25 time 5:1 22:3,11 29:3 30:25 60:14 61:1 66:15 81:18, 23 86:18 87:18 94:3 96:22,23 98:13 104:3 108:15 127:13 130:11 135:12 times 10:16	timing 7:18 today 5:18 6:22 7:4 told 27:14 tomorrow 7:19 ton 24:23 top 29:6,16 44:19 96:17 125:16 126:12 159:21 175:1 top-level 25:14 topic 99:11 total 10:18 116:17 track 129:21 trade-off 94:13 transcript 8:2 113:19,20,24 114:4,7,13 116:1 175:23,25 transferring 88:23 Translation 141:11 treat 8:1,5,11 41:1 tree 44:14,17,18 45:9,14 46:15,17 47:22 61:16 62:14,22 63:4,13, 18 69:1,5,21 70:8, 18,24,25 71:9,20, 22,24 73:7,10 147:12 tree' 45:10 tree-specific 70:19 71:3 trees 50:17 53:18 trouble 103:4 true 85:22 Trump 104:19 trust 83:10,11,17, 20,22 84:4 86:5, 12 102:9	trusted 156:8 158:6,23 truth 5:8 6:22 turn 10:24 11:3 22:12,15 43:22 110:18 121:20 139:18 152:11 153:9 155:22 174:21 type 16:2 20:6 types 17:8 typical 40:24 123:14 139:12 typically 123:17 125:21 126:19 138:7,24 139:7,13 typo 101:6 U uh-huh 51:4 52:22,25 57:12 100:22 110:22 111:14 133:17 139:21 149:15 156:1,11,14 161:19 164:25 165:21,23 177:2 181:23 ultimate 77:22 unchanged 66:3 68:7 underneath 44:20,21 understand 6:24 7:4 9:18 24:15 46:18 47:20 54:18 55:18 60:22 67:16 73:24 75:4 77:23 97:7 104:5 112:22 121:22 124:11 162:19 163:16 181:17 184:21 185:21 understanding 9:7 12:24 25:20, 22 41:18 58:18 185:5
---	---	--	--	--

understood 22:9 28:12 36:21 98:17 103:21	uploading 42:12 58:7 110:5 144:23 145:1 147:10	Verisign 86:11, 22	Wenke 5:2,6,17 25:10 35:17 86:10	23 19:12 80:16 82:11 92:5
unencrypt 142:6 144:4 145:20 146:23	uploads 58:19 67:4 68:4 69:3 71:7	version 12:2 43:5 45:10,13,16	Wenke/ documents/foo 36:13,14	writing 12:1,5
unencrypted 58:14,20 59:15,22 60:24 66:18 67:5 68:2,6,10 69:3 70:4 71:7,8 137:9 175:18	URL 17:11,17,20, 22 18:2,12,13,25 19:2,8,15,21 20:9 21:8,14,19,23 23:17,21 24:17,18 26:10 27:3	versions 108:13, 18,19	whichever 138:18	written 11:20,21 32:18 164:3
unique 25:6 26:9, 10 31:19 34:3,5 35:3,8,14,17,20, 24,25 36:10 37:9, 11,16 38:10,13, 21,23,24,25 39:1, 9 40:4,10,14 41:1 118:17,20	URLS 22:25 23:2, 10 24:9,13,17 25:5,6,8,18,23 26:8	versus 16:6 75:1 102:19 108:18 182:15	window 26:17 28:18	wrong 25:21 27:8 28:21 100:17 101:1 147:16
uniquely 23:16, 21 24:2,3 39:9,17 40:18 41:6 122:15	user 20:21,22 48:17 58:19,25 59:4 66:22 67:1,4, 12,17,23 68:4 69:2 71:7 72:9,12 73:14,24 94:17,18 140:4,8 141:1 145:8 165:18 166:4 169:1,5,13 170:8,12,22 172:11	view 70:20,23 185:4	withdraw 21:11 70:4 145:23 164:16 170:9	wrote 12:3 91:12, 24 132:10
unit 88:9	users 46:16 47:22 130:15 161:11,17,21,25 162:12,21,22 163:8 164:14,23 168:9 171:3	views 15:6	word 11:15 12:24 64:10 82:1 96:21 97:22 112:20 113:21 114:11,20 115:18 116:17,22 119:7,10 125:4 129:13 130:15 131:9 142:14,18 173:14,15 176:16 178:6 180:4,6,18, 20 181:4,6 183:4, 6	www.facebook. com 23:4
universal 17:15 26:11	valid 18:4,5,13 19:2,10,11,15 21:8,14 86:19	virtual 58:4	words 112:19 113:22,23 114:8 141:6 175:10,13, 17,19,24 176:12, 21 178:13 180:16, 24 182:7,9,10,13 183:5	www.facebook. com/2008. 26:6
universe 36:18, 19	variables 34:1	virus 106:25	work 10:1 83:18 108:22 141:2 185:13	www.google. com 17:20
unlike 93:15	vector 97:2	visualize 165:4	workflow 144:13, 16	www.w3.org/ 1999/02/22-rdf- syntax- 25:24
unlock 89:16 90:8 91:5 93:11, 14	vendor 58:7 59:6 66:24	vocabulary 30:7, 16,19 31:10	working 83:21	www.w3.org/ 1999/02/22-rdf- syntax-ns#. 26:20
unwarranted 161:16 164:23 168:9 169:1 171:2,5	vendors 20:20 98:15 99:3	W	works 74:12,17 85:3 125:5	XML 154:19
updates 172:21	verification 14:16 115:24	W-E-N-K-E 5:17	workshop 133:5	Y
upload 27:2 42:10 61:1 73:1 109:11 147:25 153:9 155:7,11, 14,20 174:12,13, 15	verify 83:5 86:24 105:13,19	wanted 61:11 138:21 175:7 176:6	world 46:20 113:18 134:18	year 12:9 100:18
uploaded 27:20 29:18 58:11 60:15 67:11 145:8 146:15 153:10 155:8,16 158:22		wanting 20:22	worry 67:14 83:2 90:13 102:22 152:22	Yuan 7:16 8:13, 21 9:3,13,24 10:11,12,14 13:3, 17 15:16 17:18,24 18:7 19:4,18 20:11 21:9,15 26:1,23 27:4,12, 23 28:1,10 29:2,8, 25 30:10,14 31:5 32:9 33:16 39:25 40:12 41:3,11,19 43:15 44:23 45:23 48:3 50:13 51:24 52:12 53:9 55:1
		watch 66:16	worst 77:11,12	
		ways 54:15 74:22 77:9,18 94:23 101:21 108:10 152:15	write 11:10,15,17,	
		weak 91:7,22		
		web 58:7 59:2,5 66:23 104:15,16 132:24 134:11,23		
		website 81:10		
		weeks 10:16		
		Wei 25:9 88:16 143:13		
		Wei's 35:20		
		well-known 81:3 129:2		
		well-publicized 87:1		

56:8 57:22 58:22
59:17 61:4 62:3,
15 63:15 64:5
66:10 68:11 69:9
70:9 71:14 72:10
75:16 77:16 78:7
79:13 80:3 82:19
87:13 89:7 91:2,
17 92:8 93:6 95:7
96:2,16 98:1
106:3,11 109:1,5
111:17 112:1
114:1,15 115:7
116:23 120:7
123:10,21 124:14
125:24 127:25
128:16 131:5,22
132:3,12,18
133:14 136:3
137:14 139:5
140:13 142:19
145:5,12 146:25
148:14 149:3,19
151:8,16 154:1
157:5 160:7
161:23 162:24
163:22 166:6
167:23 170:17
171:11 172:16
173:2,25 176:4
177:18 178:15,22
179:16 180:10
181:11 184:23
186:3,6,9