



Planet Depos®
We Make It *Happen™*

Transcript of John Black, Jr., Ph.D. (IPR2023-00458)

Date: April 3, 2024

Case: Netskope, Inc. -v- Fortinet, Inc. (PTAB)

Planet Depos

Phone: 888.433.3767

Email: transcripts@planetdepos.com

www.planetdepos.com

WORLDWIDE COURT REPORTING & LITIGATION TECHNOLOGY

Netskope Exhibit 1025

1 UNITED STATES PATENT AND TRADEMARK OFFICE

2 _____
3
4 BEFORE THE PATENT TRIAL AND APPEAL BOARD

5
6 NETSKOPE, INC.,

7 Petitioner,

8 vs.

9 FORTINET, INC.,

10 Patent Owner.
11 _____

12 PTAB Case No. IPR2023-00458

13 U.S. Patent No. 9,280,678
14

15 DEPOSITION OF JOHN BLACK, JR., Ph.D.

16 Wednesday, April 3, 2024

17 3:06 p.m. EST
18

19 Job No.: 531921

20 Pages: 1 - 97

21 Stenographically Reported By:

22 Alison C. Webster, CSR-6266, RPR, RMR, CRR, RDR

1
2
3
4 Deposition of JOHN BLACK, JR., Ph.D., produced as a
5 witness at the instance of the Petitioner, and duly sworn,
6 was taken in the above-styled and numbered cause on Friday,
7 March 22, 2024, from 3:06 p.m. to 6:56 p.m. Eastern Time,
8 before Alison C. Webster, RPR, CRR, RMR, RDR, CSR-6266
9 (Michigan); License No. 14559 (California); License No.
10 084.004953 (Illinois); License No. 23001848 (Washington),
11 reported by stenographic method, via videoconference,
12 pursuant to the Federal Rules of Civil Procedure and the
13 provisions stated on the record or attached hereto.

A P P E A R A N C E S

APPEARING ON BEHALF OF THE PETITIONER

BABAK TEHRANCHI, ESQUIRE

WEI YUAN, PH.D., ESQUIRE

Perkins Coie LLP

11452 El Camino Real

Suite 300

San Diego, California 92130

858.720.5734

btehranchi@perkinscoie.com

wyuan@perkinscoie.com

APPEARING ON BEHALF OF THE PATENT OWNER

QUINCY LU, ESQUIRE

Quinn Emanuel Urquhart & Sullivan, LLP

1109 First Avenue

Suite 210

Seattle, Washington 98101

206.905.7000

quincylu@quinnemanuel.com

T A B L E O F C O N T E N T S

Witness	Page
---------	------

JOHN BLACK, JR., Ph.D.	
------------------------	--

EXAMINATION	
-------------	--

BY MR. TEHRANCHI:	6
-------------------	---

EXAMINATION	
-------------	--

BY MR. LU:	94
------------	----

E X H I B I T I N D E X

Exhibit	Page
---------	------

(Exhibits not offered.)

1 DEPOSITION OF JOHN BLACK, JR., Ph.D.

2 Wednesday, April 3, 2024

3
4 STENOGRAPHER: The attorneys participating
5 in this deposition and the witness have verified that
6 he is John Black, Jr., Ph.D. In lieu of an oath
7 administered in person, the witness will visually
8 affirm his testimony in this matter is under penalty
9 of perjury.

10 The parties and their counsel consent to
11 this arrangement and waive any objections to this
12 manner of reporting or admissibility of the
13 transcript.

14 Would counsel please state their appearance
15 and any objections to proceeding in this manner,
16 starting with scheduling counsel.

17 MR. TEHRANCHI: Babak Tehranchi, counsel
18 for petitioner Netskope, and I have no objections.

15:05:35

15:05:37

19 MR. LU: Quincy Lu, counsel for patent
20 owner Fortinet. I have no objection.

15:05:41

15:05:44

21 STENOGRAPHER: Dr. Black, would you please
22 raise your right hand.

1 Do you swear or affirm the testimony you
2 are about to give in this matter will be the truth,
3 the whole truth, and nothing but the truth?

4 JOHN BLACK, JR., Ph.D.,
5 was thereupon called as a witness herein, and after
6 having first been duly sworn to testify to the truth,
7 the whole truth and nothing but the truth, was
8 examined and testified as follows:

9 THE WITNESS: I do. 15:06:00

10 STENOGRAPHER: Thank you. 15:05:06

11 You may proceed. 15:05:32

12 MR. TEHRANCHI: Thank you. 15:05:32

13 EXAMINATION 15:05:32

14 BY MR. TEHRANCHI: 15:05:32

15 Q. Dr. Black, today we are gonna walk through some 15:06:02

16 sections of your declaration and some of the exhibits 15:06:06

17 that are already part of the record. And just wanted 15:06:09

18 to clarify that when I refer to your declaration, it 15:06:14

19 is your supplemental declaration, Exhibit 2003. 15:06:16

20 Because I understand you had an earlier declaration, 15:06:22

21 but I'll just talk through with you with your -- with 15:06:25

22 Exhibit 2003. 15:06:30

1	A.	Understood.	15:06:31
2	Q.	And, also, if anything is unclear, please make sure	15:06:32
3		that you ask further questions. I hope, you know, we	15:06:39
4		could have a conversation that everything's clear for	15:06:41
5		the record. And if for any reason you need to take a	15:06:44
6		break, please let me know.	15:06:49
7	A.	Sounds good.	15:06:52
8	Q.	All right. Thank you.	15:06:53
9		With that, you do have a copy of your	15:06:57
10		declaration, Exhibit 2003; is that right?	15:07:01
11	A.	I have that in front of me, yes.	15:07:06
12	Q.	Okay. Great. Do you have any corrections that you	15:07:08
13		would like to make before we start this deposition;	15:07:16
14		typos, substantive issues that you would like to	15:07:19
15		correct?	15:07:23
16	A.	I didn't anticipate having an opportunity to make	15:07:26
17		corrections so I didn't write them down. I have	15:07:29
18		noticed a couple of typographical errors, or I think	15:07:31
19		one part I said the wrong ciphertext corresponded to	15:07:35
20		the wrong plaintext. And it was -- I used the	15:07:39
21		wrong -- the wrong ciphertext out of the patent spec,	15:07:42
22		or "Ronn," R-o-n-n. It should have been a different	15:07:46

1	one.	15:07:49
2	I don't think it is going to matter that	15:07:49
3	much to fix those kinds of things but I did notice a	15:07:51
4	few mistakes.	15:07:55
5	Q. Okay. If you think it matters, it affects the	15:07:55
6	substance of your declaration, you know, during the	15:07:58
7	break, one of the breaks, you may want to find out	15:08:01
8	where it is and let us know. If it's just typos and	15:08:03
9	things that are not substantive then I don't think we	15:08:07
10	need to correct it, but it's totally up to you.	15:08:09
11	A. Okay. Thank you.	15:08:12
12	Q. All right. So with that, let's go to paragraph 33 of	15:08:13
13	your declaration.	15:08:19
14	A. I'm there.	15:08:23
15	Q. And this is a fairly long paragraph. You know, feel	15:08:24
16	free to read all of it, but I'd like to focus on the	15:08:30
17	last sentence that starts with, "As the '678 patent	15:08:34
18	explains"...	15:08:37
19	Could you read that, and then I'll have a	15:08:41
20	follow-up question.	15:08:44
21	A. Okay. I read that last sentence.	15:08:52
22	Q. Okay. And that sentence says that the policy defines	15:09:10

1 multiple things; is that correct? 15:09:16

2 A. That's correct. That's in the sentence. I think 15:09:19

3 it's also in the claim, first claim of the patent as 15:09:22

4 well. 15:09:24

5 Q. Okay. And in that -- in that sentence, again in your 15:09:26

6 paragraph 33, I'm seeing six items, maybe five because 15:09:30

7 one of them may be duplicative. It talks about 15:09:36

8 accessing, processing the content, configuring the 15:09:39

9 mode in which the data is encrypted, stored, searched, 15:09:44

10 and again repeats access. 15:09:48

11 So there are basically five or six separate 15:09:51

12 items that are listed there; is that correct? 15:09:54

13 MR. LU: Objection. Vague. 15:09:58

14 A. Yeah, something like that. It's not clear exactly 15:09:59

15 what the boundaries of each of these is. Like you 15:10:13

16 said, there's maybe some overlap, but I think I 15:10:16

17 counted five or six different things. 15:10:19

18 BY MR. TEHRANCHI: 15:10:20

19 Q. Okay. But is it clear that at least you have to 15:10:21

20 access and process based on the policy. It defines -- 15:10:24

21 let me just read it so there is no ambiguity. 15:10:29

22 So it says, "...the Gateway may assign 15:10:33

1 users a policy that 'not only defines the manner in 15:10:37
2 which the users can access and process content stored 15:10:40
3 on the cloud, but can also configure...' And then 15:10:43
4 there are other things listed. 15:10:46

5 So the policy needs to define the manner 15:10:48
6 that the content is accessed and the manner in which 15:10:53
7 the content is processed. Correct? 15:10:58

8 A. Right. I think access rights are explicitly in the 15:11:02
9 policy. And then process, you know, maybe it -- that 15:11:05
10 could be almost anything. But, sure, it does say the 15:11:09
11 word "process" there. 15:11:13

12 Q. Okay. So by looking at that policy, how can you tell 15:11:14
13 which section of the policy deals with accessing, 15:11:20
14 which section of the policy deals with processing, 15:11:24
15 which section deals with encryption, storing, and the 15:11:28
16 other items that are described? So how do you know 15:11:33
17 which -- how to -- which section of the policy defines 15:11:35
18 which action? 15:11:40

19 MR. LU: Objection. Vague. Incomplete 15:11:41
20 hypothetical. 15:11:46

21 A. So, for example, if you have a policy that says, here 15:11:46
22 are the access rights. Right? So typical security 15:11:51

1 systems will say things like, you're able to read
2 these files right to those, perhaps execute under
3 certain conditions. So the access rights are
4 embodied in some standard encoding.

5 And as you know as a security person,
6 there's a whole bunch of different systems that do it
7 in a whole bunch of different ways, but we have a
8 general idea of what does it mean to give access
9 rights to a user.

10 And then separate from that, the matter in
11 which data are encrypted, that could be the algorithm
12 used for encryption, the key length restrictions, or
13 maybe even the key itself or where to find it. So
14 things related to how data are encrypted.

15 How are data stored, that could be a list
16 of cloud vendors or names of buckets in Amazon S3 or
17 something like this, but, basically, what are the
18 storage -- the cloud storage repositories that are
19 going to be used for this user.

20 Searching, that also could define the
21 manner in which search was configured so that the user
22 understands how to search and what to search, what can

15:11:54

15:11:59

15:12:05

15:12:09

15:12:11

15:12:14

15:12:16

15:12:18

15:12:21

15:12:28

15:12:30

15:12:34

15:12:39

15:12:42

15:12:47

15:12:49

15:12:57

15:12:59

15:13:02

15:13:05

15:13:08

15:13:12

1 be searched. So at least ideally, your policy would 15:13:16
2 have distinct sections indicating each of these pieces 15:13:20
3 of information. 15:13:24

4 Q. Okay. And for someone, whether gateway device or 15:13:29
5 another device or even a person, to be able to tell, 15:13:37
6 okay, I need to control access rights, how would they 15:13:41
7 know -- or I need to control where it's stored, how 15:13:46
8 would they know where to look in that policy digest or 15:13:48
9 that policy document or policy software or however 15:13:52
10 it's stored? 15:13:58

11 How do they know where to look for to get 15:14:00
12 those particular access policies or storage policies? 15:14:02

13 A. So the policy in this context is basically 15:14:08
14 configuration information. It's saying how are 15:14:11
15 things set up. And sometimes, in computer science, 15:14:15
16 these configuration documents are just plaintext. 15:14:21
17 They will literally say, access rights, and then give 15:14:24
18 you RWX or something, you know, to tell you what your 15:14:29
19 rights are. 15:14:33

20 Other times, it won't be so human readable, 15:14:34
21 it will be encoded in some sort of XML format or even 15:14:37
22 in some head-scratching binary encoding that really is 15:14:41

1 intended only for another computer to be able to 15:14:46
2 digest and understand, and a human being looking at 15:14:49
3 the configuration or the policy might really have no 15:14:52
4 clue as to how to understand its contents. 15:14:56

5 Q. And in case when something happens and that policy 15:15:00
6 needs to be changed, how would somebody change -- 15:15:04
7 let's say -- let's give an example so we're more 15:15:09
8 specific. 15:15:12

9 Let's say the encryption is broken. You 15:15:13
10 know, it's -- and it can be attacked, so you want to 15:15:19
11 use a different encryption scheme. How would you 15:15:22
12 reflect that change in the policy? 15:15:27

13 A. So if I understand your question, you're saying that 15:15:32
14 the algorithm itself is shown to be faulty and, 15:15:34
15 therefore, the company desires to replace it with 15:15:37
16 what they believe to be a better option. 15:15:41

17 So let's say AES-128 is broken and the 15:15:45
18 company says, Oh, my gosh, you know, all of our 15:15:50
19 documents over here are being encrypted with this and 15:15:53
20 we need to change that. You would have to undertake 15:15:56
21 both the task of re-encrypting everything under, let's 15:15:59
22 say, AES 256, and then you would have to update all of 15:16:04

1 the policy documents to say this user is now going to 15:16:08
2 use AES 256 as their encryption algorithm to access 15:16:11
3 those files over there because they've been 15:16:16
4 re-encrypted under that new algorithm. 15:16:18

5 Q. Okay. And I'm assuming a similar process would be 15:16:23
6 needed if the storage policy has changed. So, for 15:16:25
7 example, if Box is infiltrated and it's not safe 15:16:29
8 anymore and you want to remove it from, you know, a 15:16:34
9 remote server location to be -- for storing your data, 15:16:37
10 then how would you reflect that change in your policy? 15:16:42

11 A. You would have to move the files away from the 15:16:48
12 compromised storage repository and then you would 15:16:51
13 update the list of repositories in the policy to say 15:16:55
14 that this user now no longer has access to Box, or 15:16:59
15 whoever, but now has access to this new place where 15:17:03
16 the file chunks reside. 15:17:07

17 Q. Thank you. One other question about the policy. This 15:17:13
18 is a user policy, and I think the claim also recites a 15:17:19
19 user policy or a policy assigned to the user. 15:17:26

20 We can go to the language of the claims to 15:17:28
21 be exact. Let me go and actually make sure there is 15:17:31
22 no ambiguity in my question. 15:17:34

1 So Claim 1 says, a policy for -- assigning 15:17:38
2 to one or more users, by a gateway device, a policy 15:17:46
3 for managing access and processing a file to be stored 15:17:50
4 on one or more cloud platforms. 15:17:56

5 So the question is, those policies assigned 15:17:58
6 to a user. Correct? 15:18:04

7 A. Right. I guess to one or more, but certainly to one 15:18:06
8 user is included in that. 15:18:08

9 Q. Okay. And can it be assigned to a group of users or 15:18:14
10 class of users? 15:18:17

11 MR. LU: Objection. Incomplete 15:18:20
12 hypothetical. 15:18:25

13 A. I don't know that any of the embodiments or examples 15:18:25
14 include sort of a group management and then assigning 15:18:29
15 to a single policy to a group. So the way that I 15:18:34
16 read the claim, is that it's assigning to -- well, it 15:18:37
17 says "one or more users," and so I am -- there's 15:18:44
18 nothing that I recall from the specification about 15:18:51
19 group management where you build groups of users and 15:18:57
20 then assign policies to groups. 15:18:59

21 I would have to think about whether -- 15:19:01
22 let's say you had a system where you had groups of 15:19:03

1 users and that system assigned a policy to a group 15:19:05
2 which was comprised of users, would that satisfy the 15:19:11
3 claim limitation to one or more users, like in a 15:19:14
4 transitive way. Right? I assigned it to the group, 15:19:20
5 but the group has users, and so I, therefore, have 15:19:24
6 assigned that policy to the users belonging to the 15:19:27
7 group. I don't think I've considered that and I would 15:19:30
8 have to think about it. 15:19:33
9 Q. So let me ask you this: Does the claim prohibit 15:19:34
10 assigning the policy to a group of users? 15:19:42
11 A. I mean, it certainly doesn't say -- 15:19:46
12 MR. LU: Sorry, objection. Beyond the 15:19:48
13 scope. 15:19:51
14 A. The claim certainly doesn't say to one or more users 15:19:51
15 unless they're in a group and then don't do it. 15:19:55
16 Right? So it doesn't prohibit assigning to a group, 15:19:58
17 but once again, I'm not sure if it covers assigning 15:20:00
18 to a group. 15:20:03
19 BY MR. TEHRANCHI: 15:20:07
20 Q. Okay. And could the policy be assigned based on the 15:20:07
21 class of the user, as I alluded to earlier? And by 15:20:14
22 that I mean, mobile device users versus, you know, 15:20:20

1	P.C. users, as an example.	15:20:24
2	MR. LU: Objection. Beyond the scope.	15:20:29
3	A. I mean, certainly -- the claim just requires that the	15:20:33
4	gateway device assigns policies to one or more users.	15:20:38
5	And I suppose you can make up any practice that you	15:20:42
6	like for how you do that, as long as you're assigning	15:20:46
7	policies to users.	15:20:49
8	BY MR. TEHRANCHI:	15:20:50
9	Q. Okay. Let's switch gears just a little bit and just	15:20:58
10	talk about some of the broader aspects of what's in	15:21:05
11	this patent.	15:21:10
12	Have you -- is -- have you heard of	15:21:13
13	searchable encryption prior to reading this patent?	15:21:17
14	A. Certainly, probably in the '90s.	15:21:24
15	Q. Okay. So just having a searchable encryption	15:21:26
16	methodology or scheme is not new; is that correct?	15:21:33
17	MR. LU: Objection. Vague.	15:21:40
18	A. The concept of just being able to search encrypted	15:21:43
19	data is -- was known before the filing date of the	15:21:45
20	patent.	15:21:48
21	BY MR. TEHRANCHI:	15:21:52
22	Q. Okay. And by that -- and let's be a little bit more	15:21:52

1 clear. By searchable encryption -- searchable 15:21:55
2 encrypted data, what we mean is -- and correct me if 15:21:59
3 I'm wrong, I'm just trying to get the understanding 15:22:03
4 from your perspective. 15:22:05

5 What searchable encrypted data means is, 15:22:07
6 you can search the encrypted data without decrypting 15:22:11
7 that content; is that correct? 15:22:14

8 MR. LU: Objection. Vague. 15:22:17

9 A. I have seen the term used in all kinds of different 15:22:19
10 ways, but typically the good systems -- I've seen 15:22:23
11 papers submitted to conferences where they kind of 15:22:32
12 cheat and decrypt portions as they're searching, but 15:22:34
13 the general notion is that you want to be able to 15:22:39
14 perform a search on data that's encrypted without 15:22:42
15 decrypting in order to search. 15:22:46

16 BY MR. TEHRANCHI: 15:22:51

17 Q. Okay. And in your view, what's disclosed in the '678 15:22:51
18 patent goes beyond that basic scheme of providing 15:23:02
19 searchable encrypted contents; is that correct? 15:23:06

20 A. In the sense that it's narrower, right, that it 15:23:12
21 actually requires that this searchable encryption 15:23:15
22 scheme be implemented according to certain parameters 15:23:20

1	or limitations.	15:23:22
2	Q. Okay. So let's go to paragraphs 37 and 38 of your	15:23:28
3	declaration. And please let me know when you're	15:23:44
4	there.	15:23:55
5	A. I just arrived. I am there.	15:23:56
6	Q. Okay. Paragraph 37 is fairly short, and could you	15:23:57
7	read that, just so that we're all on the same page,	15:24:10
8	when I refer to that paragraph, there is no confusion.	15:24:13
9	A. Okay.	15:24:17
10	Q. So the last sentence or the last part of the sentence	15:24:26
11	in the -- in paragraph 37 says that, "indices, also	15:24:33
12	referred to as keywords hereinafter, which would	15:24:41
13	typically be used as search terms in the form of	15:24:46
14	search queries are stored as filenames of the chunks."	15:24:49
15	Do you see that?	15:24:56
16	A. I do.	15:24:57
17	Q. Does '678 patent say that you always have to use that	15:24:58
18	scheme to use the search terms and store them as	15:25:13
19	filenames of the chunks?	15:25:24
20	A. No. This is -- this is describing one way of doing	15:25:27
21	it. It's an embodiment. The claim, I think, is	15:25:29
22	broader than that.	15:25:34

1 Q. Okay. Fair enough.

15:25:35

2 And when you're actually implementing the
3 scheme of putting search queries as filenames, how are
4 you actually doing that?

15:25:44

15:25:47

15:25:53

5 Let me -- let me rephrase.

15:25:54

6 Does the '678 patent describe the specific
7 details of how you would use these search terms as
8 part of filenames?

15:25:56

15:26:00

15:26:07

9 MR. LU: Objection. Vague.

15:26:11

10 A. They do a fair job. Of course, there's not code in
11 the patent. There is a paper that also gives further
12 details that's attached as Appendix A to the patent,
13 but it -- you know, it gives enough information, I
14 think, that if you asked me to code it up and you
15 gave me a week, I could implement at least one way of
16 implementing the specific system that's described in
17 the Dragonfruit paper.

15:26:12

15:26:17

15:26:20

15:26:27

15:26:31

15:26:34

15:26:38

15:26:42

18 BY MR. TEHRANCHI:

15:26:43

19 Q. Okay. Yeah, no, we don't want you to code it up for
20 us right now, but let's just -- just in words.

15:26:44

15:26:46

21 And I'm not looking for -- you know, you
22 could go into details if you like, but you have search

15:26:51

15:26:54

1	terms and then you have the file. How would you --	15:26:57
2	would you just take the search terms and make them	15:27:02
3	part of the file name?	15:27:08
4	MR. LU: Objection. Vague. The document	15:27:12
5	speaks for itself.	15:27:15
6	A. You break the file into chunks, but then those chunks	15:27:17
7	are encrypted and you distribute them to various	15:27:21
8	cloud repositories and you create these namespaces on	15:27:25
9	the various cloud repositories that hold the chunks,	15:27:30
10	and then the file names are the encrypted keywords	15:27:34
11	that you -- you indicated them in your question, you	15:27:37
12	encrypt them and put one or more of them as file	15:27:41
13	names of the various chunks.	15:27:44
14	BY MR. TEHRANCHI:	15:27:49
15	Q. So the file name could have multiple search terms in	15:27:50
16	it. Correct?	15:27:57
17	MR. LU: Objection. Vague.	15:27:59
18	Mischaracterizes testimony.	15:28:00
19	A. I'm pretty sure. I'd have to check, but I think one	15:28:04
20	of the embodiments says that you could actually have	15:28:06
21	multiple search terms concatenated or included in a	15:28:10
22	single file name.	15:28:13

1	BY MR. TEHRANCHI:	15:28:19
2	Q. And what happens -- okay. Scratch that.	15:28:19
3	Can you have -- is there any limits on the	15:28:21
4	number of search terms that you can have in this	15:28:24
5	scheme?	15:28:29
6	MR. LU: Objection. Vague.	15:28:31
7	A. When you create the name space, you are going to have	15:28:34
8	some kind of limits on what can be contained as	15:28:37
9	values. Now, in the terms of the specific	15:28:42
10	implementation we're talking about, virtually every	15:28:45
11	file system has a length limit on file names, so that	15:28:48
12	would be a constraint. You couldn't put so many	15:28:52
13	keywords in a file name that you would then exceed	15:28:55
14	the file name limit of the file system.	15:28:59
15	There might also be certain forbidden	15:29:03
16	characters that could limit, you know, what you could	15:29:07
17	do in a file name as well.	15:29:10
18	BY MR. TEHRANCHI:	15:29:10
19	Q. Can that file name have other fields or other	15:29:21
20	information other than the search keywords?	15:29:24
21	MR. LU: Objection. Vague. Beyond the	15:29:31
22	scope.	15:29:37

1 A. I don't think in the embodiment it does. I don't 15:29:38
2 think that the claims require that when you configure 15:29:41
3 the name space to be searchable, that you're not 15:29:45
4 allowed to add other things, you know, to the name 15:29:49
5 spaces, if you like; it just needs to be configured 15:29:53
6 to be searchable. So I don't see an explicit 15:29:55
7 proscription against other data in the file name. 15:29:57

8 BY MR. TEHRANCHI: 15:30:08

9 Q. How do you know -- how do you know how the search 15:30:14
10 terms are delineated in that file name? 15:30:22

11 And let me give you a particular example. 15:30:24
12 So let's say you have three search terms that you are 15:30:29
13 making those search terms, you put it in the file 15:30:32
14 name. How do you know where each search term in that 15:30:35
15 file name begins and where it ends? 15:30:38

16 MR. LU: Objection. Vague. 15:30:43

17 A. So the way that we normally do this in a computer 15:30:47
18 implementation is we either use a separator between 15:30:50
19 terms, and that can be a character that's forbidden 15:30:53
20 from being included in the term itself, like a 15:30:56
21 vertical bar, let's say, or a comma or something that 15:30:59
22 you can't have in the search term, and that's used as 15:31:02

1 a separator. 15:31:05

2 You could also insist that the search term, 15:31:06

3 when its encrypted, have a fixed length. So even if 15:31:10

4 it's a short word, it's 20 characters long or 15:31:14

5 something like this, and so now I know where every 15:31:16

6 term begins and ends because they all have the same 15:31:19

7 length. There are various techniques like this. 15:31:23

8 BY MR. TEHRANCHI: 15:31:26

9 Q. Okay. But when somebody is searching that file name, 15:31:26

10 they are able to search based on individual file names 15:31:31

11 so they're able to somehow parse that file name and be 15:31:36

12 able to match or obtain that search term. Correct? 15:31:39

13 MR. LU: Objection. Vague. 15:31:45

14 A. That's right. So if, let's say -- I mean, the idea 15:31:46

15 in this embodiment is that we're going to leverage 15:31:51

16 the cloud's built-in ability to look through file 15:31:55

17 names quickly, so I don't have to build a separate 15:31:58

18 piece of software that parses file names. I just ask 15:32:00

19 the cloud service to use its built-in ability to look 15:32:06

20 through its file system. 15:32:10

21 So let's say I'm looking for -- let's say 15:32:12

22 I'm using vertical bars to separate my search term, 15:32:14

1 maybe there's a bunch of them in a file name. I would 15:32:17
2 say, you know, look for asterisk, meaning anything, 15:32:20
3 vertical bar, my search term, vertical bar, asterisk. 15:32:27
4 And the file system knows how to handle that query. 15:32:31
5 Right? It just says, if there's anything with these 15:32:35
6 letters between these two vertical bars, return it; 15:32:37
7 otherwise, say not found. 15:32:40
8 Q. Okay. So are you saying that the file system knows 15:32:48
9 that these are forbidden characters, and then it would 15:32:54
10 automatically say that that's where the search term 15:33:00
11 starts or ends, or is there additional logic that 15:33:04
12 needs to be added to say, well, if you see these 15:33:06
13 forbidden characters, then do these other steps to 15:33:13
14 find the search term? 15:33:17
15 A. I mean, in this -- the way that I'm imagining this -- 15:33:21
16 implementing this system, is I would just make sure 15:33:25
17 that my encryption algorithm never outputs ciphertext 15:33:28
18 with a vertical bar. 15:33:32
19 For example, if it always outputs 128 bits 15:33:34
20 and then I encode that with, you know, Base64 or 15:33:40
21 something, I'll encode it into just alphanumerics, I 15:33:44
22 won't have a vertical bar. But I would arrange that 15:33:47

1 the encrypted keywords never have the forbidden 15:33:50
2 character in it, the way that I will encode them 15:33:55
3 before putting them into file names. And then I'll 15:33:57
4 use my reserved vertical bar character, my special 15:34:00
5 character, as the limiters. 15:34:03
6 The file system doesn't have to know what 15:34:04
7 I'm up to at all. It just needs to know how to be a 15:34:06
8 file system, how to look up things with wild cards. 15:34:11
9 Q. Okay. So in that scenario, when a search query -- and 15:34:14
10 I'm assuming it's an encrypted search query that goes 15:34:20
11 to the cloud storage device -- then what -- is there 15:34:23
12 any additional logic that is needed for that cloud 15:34:31
13 storage device to know that, well, you have to look 15:34:34
14 for delimiters and you have to look for multiple 15:34:38
15 delimiters to know where things start and end or 15:34:42
16 any -- or can you just implement this as it is on any 15:34:45
17 cloud storage device out there, without adding any 15:34:50
18 additional logic? 15:34:52
19 A. Yeah, in this embodiment we're not going to ask 15:34:58
20 Amazon to, you know, augment its service at all. 15:35:00
21 It's just a file system. And all of the searchable 15:35:03
22 encryption technology is being done by me, and I'm 15:35:08

1	just asking it, hey, could you store the file, and	15:35:15
2	here's its name.	15:35:18
3	And then when I look it up later, you	15:35:19
4	know, just be able to -- just be able to look up	15:35:21
5	asterisk vertical bar 123 vertical bar asterisk, and	15:35:24
6	tell me, does any file have that vertical bar 123	15:35:29
7	vertical bar anywhere in any file name anywhere in	15:35:33
8	this folder or in this container.	15:35:35
9	Q. So your search query that you're sending to the cloud	15:35:37
10	storage needs to have the delimiters as part of the	15:35:41
11	search query.	15:35:43
12	MR. LU: Objection. Mischaracterizes	15:35:44
13	testimony.	15:35:45
14	A. I mean, if I'm going to choose delimiters in this	15:35:50
15	implementation that I'm imagining, then, of course,	15:35:53
16	the delimiters have to be valid characters for file	15:35:56
17	names for that cloud provider. If they're not, I'll	15:35:59
18	choose a different one. But the cloud provider	15:36:03
19	doesn't need to know that I'm using a particular	15:36:05
20	character as a delimiter; as far as it's concerned,	15:36:08
21	it just has a string of characters that's a file name	15:36:09
22	and it has some contents, that's the file contents,	15:36:12

1 and it doesn't care about what I'm doing with any of 15:36:15
2 that stuff. 15:36:17

3 BY MR. TEHRANCHI: 15:36:18

4 Q. Understand. But again, going back to that search 15:36:18
5 query that, in this scenario, you would have to have 15:36:22
6 those delimiters in that search query; is that 15:36:25
7 correct? 15:36:29

8 A. Yeah, the way that I'm imagining it, you know, if you 15:36:31
9 didn't include the delimiters you might get the wrong 15:36:36
10 answer. 15:36:38

11 Like, you indicated -- I think you were 15:36:42
12 hinting before, you know, if I have a encrypted 15:36:44
13 keyword that begins in an A and I have another one 15:36:47
14 that starts with a B and I put them together, and I 15:36:51
15 look for A-B, I might get part of the first one with 15:36:53
16 part of the second one and get mixed up and get a 15:36:56
17 wrong result, which is why I said you would want to 15:36:59
18 make sure that you kept them delimited separate. 15:37:03

19 Q. And as you mentioned before, you mentioned -- correct 15:37:22
20 me if I'm wrong -- that there are certain -- there 15:37:27
21 could be certain forbidden characters that you cannot 15:37:30
22 add to the file name. So when you are encrypting your 15:37:37

1 search terms, then you have to do something to make 15:37:46
2 sure that those forbidden characters are not present; 15:37:48
3 is that correct? 15:37:51

4 MR. LU: Objection. Vague. 15:37:53

5 A. Right. So normally when you encrypt, say, using AES, 15:37:53
6 you're going to get 128 bits output. And you're not 15:37:59
7 going to use those bits as a file name, it's going to 15:38:03
8 be binary and it's going to gobbledygook if you try 15:38:06
9 to print it. So typically what we do is we then 15:38:11
10 encode the ciphertext in some way that it's, you 15:38:14
11 know, amenable to being used either in a text 15:38:17
12 document or in an email or as a file name, in this 15:38:19
13 case. 15:38:25

14 And so the binary is very, you know, 15:38:28
15 awkward to work with because a lot of places where 15:38:31
16 you would want to send it, can't receive it. So in 15:38:33
17 emails we typically use, like, MIME 64 encoding or 15:38:36
18 use Base64 encoding; in web, we use MIME encoding. 15:38:40
19 But you would do some encoding process to make it 15:38:46
20 into something printable, and also to respect 15:38:48
21 whatever the cloud storage file systems rules are. 15:38:54

22 If they say you can't have a slash in a 15:38:57

1 file name, then you have to encode it in such a way 15:38:59
2 that avoids a slash. So that's up to you, before you 15:39:02
3 send the file to the cloud service, to make sure 15:39:05
4 you're abiding by all the rules that the file system 15:39:07
5 has. 15:39:10

6 Q. And those modifications or those considerations to 15:39:15
7 generate these search terms for different -- would it 15:39:19
8 be different for different cloud storage systems? 15:39:25

9 MR. LU: Objection. Incomplete 15:39:31
10 hypothetical. Vague. 15:39:34

11 A. If I were implementing it, probably not. I would 15:39:35
12 just pick an encoding system that was going to be 15:39:37
13 gentle enough and not very demanding, wouldn't have a 15:39:42
14 lot of special characters. I wouldn't encode 15:39:47
15 something that has asterisks in it because that might 15:39:50
16 confuse a Windows-based system, perhaps. 15:39:54

17 So if you're just very generic, use upper, 15:39:57
18 lowercase letters, and maybe 039, stay away from 15:39:59
19 punctuation, then you probably don't need to worry 15:40:03
20 about the rules that the file system has. 15:40:07

21 If you wanted to push the envelope and say, 15:40:09
22 well, I really want to allow, like, slashes and 15:40:11

1 backslashes and other things that certain vendors 15:40:14
2 might be sensitive to, now you might have to, like, 15:40:17
3 change your scheme based on which cloud service you're 15:40:20
4 using, but I think that's a bad engineering choice. 15:40:23
5 Q. You may have alluded to this earlier as well. So 15:40:26
6 introducing these encrypted search indexes or 15:40:54
7 keywords, you can use different encryption schemes 15:41:02
8 that could be -- you could have a fixed output length, 15:41:08
9 you could have a variable length output; is that 15:41:11
10 correct? 15:41:14
11 A. Yeah, there are options on how you implement things. 15:41:17
12 Q. And that -- based on your opinion, the claims for the 15:41:22
13 patent do not restrict the invention or the claims to 15:41:28
14 one type or another; is that correct? 15:41:33
15 MR. LU: Objection. Vague. 15:41:38
16 A. Certainly the independent claims don't. There 15:41:40
17 might -- might be a dependent claim somewhere that 15:41:44
18 has more restrictions on how it's done. I don't 15:41:48
19 recall anything that says variable length versus 15:41:52
20 fixed length, specifically. 15:41:54
21 BY MR. TEHRANCHI: 15:41:56
22 Q. So I think that's a nice segue to your paragraph 38. 15:41:58

1 And -- I mean, this is a little bit longer paragraph, 15:42:05
2 but I'm going to ask questions about the second part 15:42:13
3 of it that goes to your page -- your page 14, and I 15:42:18
4 think this is an example that you have reproduced from 15:42:24
5 the -- from the '678 patent that the search term 15:42:27
6 "Ronn" is encrypted by the gateway to generate a 15:42:34
7 ciphertext "uetywo." Do you see that? Is that 15:42:40
8 correct? 15:42:47
9 A. It's correct it says that. I think that may be an 15:42:50
10 example of where I got ciphertext wrong, but it does 15:42:53
11 say that in my report. 15:42:56
12 Q. Okay. And the question that I have is, "Ronn" is a 15:42:58
13 four-letter word and "uetywo" is a six-letter word. 15:43:04
14 Do you see that? 15:43:10
15 A. That's true. 15:43:15
16 Q. Okay. So is it generally correct that the ciphertext 15:43:16
17 does not need to be the same length as your plaintext? 15:43:21
18 A. Yes, that's true. And, in fact, the correct 15:43:28
19 ciphertext in the patent, had I not made that typo, 15:43:30
20 is also six letters. So, again, it's going from four 15:43:36
21 letters to six letters. 15:43:39
22 Q. Based on your knowledge in this area, do you consider 15:43:54

1 an encryption that produces a ciphertext of -- that is 15:43:59
2 six letters long, is that considered a strong 15:44:04
3 encryption? 15:44:07

4 MR. LU: Objection. Vague. 15:44:11

5 A. No. The concept of strong encryption has nothing to 15:44:12
6 do with lengths of the ciphertext. 15:44:16

7 BY MR. TEHRANCHI: 15:44:19

8 Q. How easy would it be to get -- reverse engineer the 15:44:24
9 ciphertext to get the plaintext? 15:44:30

10 MR. LU: Objection. Vague. Incomplete 15:44:33
11 hypothetical. 15:44:40

12 A. That's a deep question. So to reverse engineer, one 15:44:40
13 way to do it would be to just have your plaintext 15:44:52
14 ciphertext pair and then do a brute-force key search, 15:44:57
15 assuming you know the algorithm. 15:45:02

16 We usually assume, in cryptography, that 15:45:04
17 we know the algorithm that's being used, that's not 15:45:06
18 hidden. If it is hidden, that's called security by 15:45:09
19 obscurity, and we frown on that. 15:45:14

20 So let's say, in your question, we know 15:45:15
21 the algorithm that's being used, we don't know the 15:45:17
22 key, and we have an example of a plaintext and a 15:45:20

1	ciphertext. Now, we can try to brute-force the key	15:45:22
2	by just trying all possible keys. How hard that is	15:45:29
3	would depend on the size of the key space.	15:45:32
4	So if you have a 16-bit key, it's trivial.	15:45:34
5	If you have 128-bit key, it's probably more than our	15:45:41
6	lifetime, even with a very fast computer. So if	15:45:44
7	that's the sense in which you're trying to	15:45:47
8	brute-force it, it's going to take a very long time.	15:45:50
9	But there are other ways you could try to	15:45:53
10	brute-force the ciphertext as well. If you have the	15:45:57
11	black box that has the key embedded and you're	15:45:59
12	allowed to -- a chosen plaintext attack, which means	15:46:02
13	you're allowed to submit plaintexts and see if you	15:46:06
14	get the same ciphertext that you're searching for,	15:46:08
15	that's a different type of attack.	15:46:11
16	So it depends, I suppose, when you said how	15:46:13
17	hard would it be to brute-force the ciphertext.	15:46:15
18	Q. Okay. Fair enough.	15:46:22
19	Okay. So let's go to your paragraph 39.	15:47:10
20	A. Okay.	15:47:17
21	Q. And that paragraph concludes with, I think, one long	15:47:18
22	sentence that says, "This novel process provides	15:47:24

1	multiple benefits over the prior art encrypted	15:47:27
2	indices..."	15:47:32
3	And number one, you say, "search being	15:47:33
4	performed by a powerful hardware of the cloud service	15:47:36
5	instead of the gateway device or a user device."	15:47:39
6	And then number two is, "search not being	15:47:41
7	limited to a device that hosts the index - any device	15:47:44
8	can perform the query, as the keywords are encrypted	15:47:49
9	using a public key."	15:47:52
10	So one question is, do you have to perform	15:48:02
11	the query -- or do you have to encrypt the keywords	15:48:04
12	using public key?	15:48:09
13	MR. LU: Objection. Vague.	15:48:12
14	A. Your question is, if I'm going to perform a search on	15:48:14
15	the encrypted data, do I have to use public-key	15:48:18
16	cryptography as opposed to symmetric-key cryptography	15:48:22
17	to do that?	15:48:26
18	BY MR. TEHRANCHI:	15:48:27
19	Q. That's correct.	15:48:28
20	A. I think that the patent covers both types of	15:48:34
21	encryption. Certainly the sentence you read applies	15:48:37
22	in either case. It doesn't say you have to use	15:48:44

1 public key. So my answer is, no, you don't have to 15:48:46
2 use public-key cryptography to do this. 15:48:49

3 Q. But let me rephrase the question or have a different 15:48:52
4 question. 15:48:55

5 In cases where you do not use public-key 15:48:57
6 cryptography, if you use asymmetric-key algorithm, for 15:49:02
7 example, do you still benefit from Item Number 2 that 15:49:05
8 is listed in -- that you are describing in your 15:49:10
9 paragraph 39? 15:49:13

10 A. I see. I missed what the end of the paragraph 15:49:25
11 actually stipulates, a public key in that example. 15:49:29

12 So in that example, it's saying that the 15:49:32
13 keywords are encrypted using a public key. I'm just 15:49:34
14 saying that the patent also talks about using 15:49:41
15 symmetric keys in other places, but in this -- I think 15:49:42
16 in this embodiment they're saying that the keywords 15:49:45
17 are encrypted using a public key which would mean you 15:49:47
18 would need that public key to do a query. 15:49:50

19 Q. Understood. But the patent or the claims don't 15:49:52
20 require using public-key algorithm. Correct? 15:49:56

21 A. No, they just say perform encryption. They don't -- 15:50:05
22 at least Claim 1 doesn't stipulate what kind of 15:50:08

1	algorithm must be used.	15:50:11
2	Q. Also, I believe -- and I could show you where it is --	15:50:15
3	the '678 patent describes that you could download	15:50:22
4	these files locally and do the searches locally.	15:50:25
5	Do you recall seeing that?	15:50:29
6	A. I don't recall it.	15:50:34
7	Q. I think it's in one of the dependent claims. So if	15:50:36
8	you go to the patent, Exhibit 1001, Claims 2, 3, and	15:50:59
9	4.	15:50:59
10	Claim 2 says, "...the step of managing	15:51:14
11	comprises allowing [the] one or more users to download	15:51:16
12	the searchable encrypted file to a local device."	15:51:20
13	Do you see that?	15:51:25
14	A. I do.	15:51:27
15	Q. And in Claim 4, which depends from Claim 2, says,	15:51:28
16	"wherein the downloaded encrypted file is searchable	15:51:34
17	by the one or more users using the cryptographic key	15:51:36
18	information."	15:51:41
19	Do you see that?	15:51:42
20	A. I do.	15:51:43
21	Q. Okay. So based on these and -- is it -- can you --	15:51:44
22	you agree that the files, the searchable files, can be	15:51:53

1 downloaded to a local device and searched in the local 15:51:58
2 device? 15:52:01

3 A. I mean, Claim 2 clearly says that, at least in this 15:52:16
4 dependent claim, "one or more users" are allowed to 15:52:20
5 "download the searchable encrypted file to a local 15:52:24
6 device". So that would -- that would satisfy the 15:52:26
7 part of your question that says download to a local 15:52:29
8 device. 15:52:31

9 And in Claim 4, says that the encrypted 15:52:32
10 file is still searchable by one or more users. So I 15:52:36
11 suppose in that case you would still use the same 15:52:39
12 search technique but you wouldn't be able to leverage 15:52:43
13 the power of the cloud hardware anymore. 15:52:46

14 Q. Fair enough. 15:52:48

15 So the two items that -- Item 1 in your 15:52:52
16 paragraph 39, that says you leveraged the "hardware of 15:52:54
17 the cloud service," that doesn't apply to the local -- 15:52:59
18 to the scenario where you store the file locally, it's 15:53:02
19 only when you do store it in the -- outside in the 15:53:05
20 cloud provider. Correct? 15:53:10

21 A. I mean, I suppose you could still perform the search 15:53:14
22 on the cloud, even if you have the file downloaded 15:53:18

1	locally. But certainly, if you perform the search	15:53:21
2	locally you're not enjoying any power from the cloud	15:53:24
3	at that step.	15:53:26
4	Q. Okay.	15:53:28
5	MR. TEHRANCHI: You know, I'm kind of at	15:53:44
6	the end of one set of questions. This may be a good	15:53:45
7	time to take a five-, ten-minute break. It's up to	15:53:50
8	you. I can go on, but let me know, please, if you	15:53:53
9	want to have a break or you want to continue.	15:53:55
10	THE WITNESS: I'd be happy to go refill my	15:53:58
11	water glass and come back in, say, ten minutes.	15:54:00
12	MR. TEHRANCHI: Ten minutes.	15:54:03
13	(Off the record at 3:54 p.m.)	15:54:05
14	(Back on the record at 4:07 p.m.)	16:07:01
15	BY MR. TEHRANCHI:	16:07:06
16	Q. Dr. Black, let's talk a little bit about namespace.	16:07:06
17	Does the '678 patent describe what a	16:07:14
18	namespace is?	16:07:18
19	A. I think by example, but it doesn't explicitly set out	16:07:25
20	a definition that I recall.	16:07:28
21	Q. Okay. You said, "by example." Can you point to an	16:07:31
22	example where it shows or it says, this is a	16:07:36

1 namespace? 16:07:40

2 A. I thought I saw an example, but it's an example of a 16:08:24

3 storage container could be a namespace, not the other 16:08:27

4 way. 16:08:30

5 I mean, it lists things like -- I'm reading 16:08:33

6 from the patent now -- namespaces, directories, 16:08:42

7 folders, files. It doesn't define any of those, it 16:08:46

8 doesn't tell you what a directory is or a folder is or 16:08:49

9 a namespace is. It just uses the term without 16:08:53

10 definition. 16:08:56

11 Q. Okay. What is your understanding of what a namespace 16:09:00

12 is from a perspective of a person of ordinary skill in 16:09:04

13 the art in 2013? 16:09:09

14 A. A namespace is a common concept in computer science 16:09:14

15 that a POSITA would have been aware of, and I believe 16:09:20

16 that they would have understood it to mean a range of 16:09:23

17 values available in a certain context. 16:09:26

18 Q. Okay. And you said "a range of values." Is that an 16:09:30

19 example -- exclusive example or it could be a range of 16:09:42

20 other things as well? 16:09:47

21 MR. LU: Objection. Vague. 16:09:51

22 A. I mean, I think I say, in my declaration, it's a set 16:09:53

1 of names. Names are typically values or data items, 16:09:58
2 but that's a broad term that encompasses almost 16:10:04
3 anything. A name can be almost anything. 16:10:07
4 BY MR. TEHRANCHI: 16:10:09
5 Q. Okay. And does the '678 patent explain how the 16:10:09
6 namespace is created? 16:10:18
7 A. I think only through examples. They don't explicitly 16:10:26
8 say, here's the only possible way to do it. They 16:10:30
9 just create a container and say, that's a name space, 16:10:34
10 for example. 16:10:40
11 Q. Okay. Can you point me where in '678 it's providing 16:10:41
12 that example? 16:10:45
13 A. So in column 10, I'm reading from line 11 of the 16:12:16
14 '678, and they're showing -- they're saying, As can 16:12:24
15 be seen in Figure 2, one or more containers, for 16:12:26
16 example, directories, folders, files and their 16:12:30
17 associated namespaces of cloud service providers can 16:12:33
18 store metadata... 16:12:38
19 So I believe when they refer to a namespace 16:12:40
20 in the context of Figure 2, they're referring to the 16:12:42
21 containers that were created. 16:12:44
22 Q. I'm going to -- I'm looking at Figure 2, and would you 16:12:47

1 point me in Figure 2 where you think that namespaces 16:13:12
2 are created? 16:13:18

3 A. I don't think Figure 2 depicts the creation. I think 16:13:26
4 it's showing that cloud service providers can hold 16:13:29
5 information. It's the narrative that talks about 16:13:34
6 creation of a container could, for example, be a 16:13:37
7 namespace. That was in the passage I read. 16:13:41

8 Q. Okay. So let me go back to column 10, line 11. 16:13:48

9 As can be seen in Figure 2, one or more 16:13:56
10 containers, e.g., directories, folders, files, and 16:13:58
11 their associated file names of cloud service providers 16:14:02
12 can store metadata and/or content associated with 16:14:08
13 searchable encrypted files which can be accessed... 16:14:12
14 and so on. 16:14:17

15 So, Dr. Black, I don't see anything about 16:14:18
16 how those are created. All I see here is that it 16:14:21
17 has -- Figure 2 shows one or more containers such as 16:14:26
18 directories, folders, files, and their associated file 16:14:30
19 names that can store metadata and content. 16:14:34

20 So there's nothing in here that I can see 16:14:39
21 that says, this is how you would create a namespace; 16:14:43
22 is that fair? 16:14:46

1	MR. LU: Objection. Argumentative.	16:14:49
2	A. I mean, it's fair that it doesn't say, here's how you	16:14:52
3	create a namespace or here's how a cloud provider	16:14:56
4	creates a container. That is something that's	16:14:59
5	probably left up to the cloud provider themselves.	16:15:02
6	They decide on the implementation of their container	16:15:06
7	system.	16:15:10
8	So as part of creating a namespace, you're	16:15:11
9	going -- at least in some embodiments, you're going	16:15:15
10	to go out into the cloud provider and say, create	16:15:20
11	this storage bucket, this storage area, this	16:15:22
12	container, and that's part of what it means to create	16:15:24
13	a namespace in the sense that the patent's doing it.	16:15:29
14	BY MR. TEHRANCHI:	16:15:39
15	Q. So who creates -- which entity creates the namespace?	16:15:39
16	Is it the storage -- the cloud storage or is it the	16:15:43
17	gateway? Is it the user?	16:15:47
18	MR. LU: Objection. Vague.	16:15:54
19	A. I think in this example it's -- the policy is part of	16:15:55
20	what's creating it, what is stated in the policy,	16:16:00
21	because that influences the namespace; therefore, the	16:16:03
22	human author of the policy is part of that story.	16:16:06

1 And then when the action is taken to 16:16:11
2 actually go out and, you know, place file chunks and 16:16:14
3 put them on the file containers, that means that the 16:16:19
4 cloud provider is also now implicated in this story as 16:16:23
5 one of the participants in creating the namespace. 16:16:27

6 So I would say that there are a few actors 16:16:30
7 here; you know, the person or persons who wrote the 16:16:33
8 policy file, the policy file itself, and then any of 16:16:37
9 the computers between where the gateway is and the 16:16:42
10 cloud -- various cloud providers that allocate space 16:16:47
11 on their disk drives. 16:16:50

12 All of those are part of the creation 16:16:52
13 story. 16:16:54

14 Q. Can you go to your paragraph 71 of the declaration, 16:16:58
15 please? 16:17:17

16 A. I'm there. 16:17:23

17 Q. Okay. So, yeah, feel free to read that paragraph. My 16:17:24
18 question is about the last sentence that says, "Hence, 16:17:33
19 naming the folder with the encrypted filename and 16:17:36
20 storing the file chunks in that folder creates a 16:17:40
21 namespace scope for the file chunks." 16:17:44

22 Do you see that? 16:17:49

1	A.	I do.	16:17:52
2	Q.	Okay. So I realize here you say it "creates a	16:17:53
3		namespace scope for the file chunks." Is that	16:17:59
4		different from creating a namespace?	16:18:03
5	A.	Yes. Because if all you did was create the scope,	16:18:13
6		meaning the range of possible values, that's not	16:18:18
7		enough to create a namespace. But to create a	16:18:21
8		namespace, you do have to define a namespace scope.	16:18:25
9		So that's one part of what you would do to create a	16:18:27
10		namespace.	16:18:30
11	Q.	So it's not enough to create that scope, to say that	16:18:32
12		the files need to be within this range of values or	16:18:39
13		these are the range of names that can be used to name	16:18:44
14		these files. That's not enough, in your view.	16:18:47
15	A.	In my view, that would not be enough to be a	16:18:52
16		namespace in the way that the patent uses the term	16:18:56
17		because you don't -- you haven't established a	16:18:59
18		context.	16:19:01
19		So if I say, you know, filenames can be	16:19:04
20		three digit numbers, but I haven't told you in what	16:19:06
21		context, where do they live, I haven't separated them	16:19:11
22		from the global universe of all files in the world.	16:19:14

1 I haven't really created a namespace because I 16:19:18
2 haven't insulated this group of files from all the 16:19:20
3 rest of the files on the planet. I need to tell you 16:19:24
4 what the context is for these values, where do they 16:19:27
5 live, so that when I say 123, you know which one I 16:19:29
6 mean; I mean the one in this container, not in that 16:19:35
7 container. 16:19:39
8 Q. Does that mean you need to specify a directory path? 16:19:41
9 I'm not quite clear what you mean that you 16:19:43
10 have to provide a context. Can you explain that, 16:19:46
11 please? 16:19:51
12 A. Sure. So if you create a directory and say, My 16:19:52
13 namespace is going to be three-digit numbers, the 16:19:57
14 filenames will be three-digit numbers within this 16:20:02
15 directory, that directory now has become your 16:20:05
16 namespace. You've indicated what the scope is, what 16:20:07
17 the possible values are, and where those files live. 16:20:10
18 But if you hadn't included where they live 16:20:14
19 and you said, get that file 123 that's on my Windows 16:20:16
20 machine, and I say, well, there's 17 of them, right, 16:20:22
21 you haven't told me where to look. So I need that 16:20:25
22 context as well to create this space. 16:20:27

1 Space is like, you know, conceptually a 16:20:31
2 place where things live in a context so that we both 16:20:35
3 understand what we're talking about when we talk 16:20:41
4 about objects within that context. 16:20:43

5 Q. Okay. So in that example, if you are using a cloud 16:20:48
6 storage or provider to store your files, when you 16:20:56
7 create the namespace, do you have to specify the cloud 16:21:03
8 storage provider's name in addition to the location 16:21:06
9 within that cloud storage that files reside and then 16:21:12
10 the range of values of the -- of the names? All 16:21:16
11 three? 16:21:20

12 A. Yeah, maybe even more than that. Right? At least in 16:21:23
13 the -- in this implementation we're talking about, to 16:21:27
14 describe the context, you would have to indicate not 16:21:30
15 only that it's Amazon, but perhaps even which part of 16:21:32
16 Amazon because there's various places that you could 16:21:36
17 put things. 16:21:38

18 So you have to give a complete description 16:21:39
19 of where this namespace lives so that you, without any 16:21:41
20 other information, could also find it, identify it, as 16:21:46
21 well as the range of values that can live within it. 16:21:50

22 But I -- the context, I mean, in computer 16:21:53

1 science, you would have to give it a clear context, so 16:21:55
2 you wouldn't be ambiguous. 16:21:57

3 Q. So back to your paragraph 71, at the beginning of the 16:22:13
4 paragraph, you say, "The '678 patent provides an 16:22:20
5 example of creating and configuring namespaces as part 16:22:23
6 of an encryption process." 16:22:27

7 And then go on to say, "For example, the 16:22:29
8 '678 patent teaches that 'each chunk can be encrypted 16:22:32
9 based on public and private/secret keys defined by the 16:22:36
10 encryption module...where the keys are managed based 16:22:42
11 on user-assigned policies." 16:22:46

12 Do you see that? 16:22:48

13 A. I do. 16:22:52

14 Q. Okay. So is there any further explanation in the 16:22:53
15 patent that how you would go from using encryption on 16:22:57
16 each chunk, which you are describing here, to creation 16:23:05
17 of the namespace? 16:23:09

18 A. I'm sorry, I'm not sure I understand the question. 16:23:33

19 Q. Okay. So the beginning of that paragraph 71, it -- at 16:23:37
20 least to -- and correct me if I'm wrong, this is your 16:23:42
21 declaration so I don't want to, you know, say 16:23:44
22 something that is not true. 16:23:48

1 The first sentence, you are saying that 16:23:49
2 "'678 patent provides an example of creating and 16:23:51
3 configuring namespaces as part of an encryption 16:23:54
4 process." Right? 16:23:58

5 And then go on to say, for example, you 16:23:59
6 encrypt each chunk based on public and private keys 16:24:02
7 defined in encryption module and where the keys are 16:24:06
8 managed. 16:24:10

9 And you -- the next sentence also that I 16:24:11
10 didn't read, it says, therefore -- "These policies 16:24:13
11 therefore create a namespace that defines the naming 16:24:16
12 convention for the file chunks." 16:24:19

13 So my question is, again, is there anything 16:24:22
14 in '678 patent that says, based on encryption of the 16:24:28
15 files, of the chunks, you are creating a namespace? 16:24:34
16 Is there a connection made there? 16:24:39

17 How -- in other words, how would you do 16:24:41
18 that based on '678? 16:24:43

19 MR. LU: Objection. Vague. 16:24:47

20 A. In your question, "how would you do that," what do 16:24:48
21 you mean, "how would you do" -- what's the "that" 16:24:51
22 part? 16:24:53

1	BY MR. TEHRANCHI:	16:24:54
2	Q. You know, this is your -- your statement. Right? So	16:24:55
3	I'm assuming this paragraph provides an explanation of	16:24:59
4	how the namespace is created.	16:25:04
5	So could you, in your own words, explain	16:25:08
6	how they're created based on what you are saying in	16:25:11
7	that paragraph?	16:25:15
8	I mean, if there are additional things that	16:25:16
9	you're not saying there, that's fair, we can go there.	16:25:18
10	But my first question is, based on what you've stated	16:25:20
11	here, how are namespaces created?	16:25:23
12	A. The namespace is created -- once again, the full	16:25:28
13	story starts with, you know, writing the policies	16:25:31
14	that indicate where things are going to be stored,	16:25:34
15	what encryption algorithms are going to be used,	16:25:37
16	perhaps the keys are in the policy as well. Whoever	16:25:39
17	decides all of that plays the first step in the	16:25:43
18	creation of the namespace.	16:25:48
19	And then, as I say here, the chunks are	16:25:50
20	encrypted based on --	16:25:54
21	Q. Can I interrupt you for a second?	16:25:56
22	A. Go ahead. For sure.	16:25:58

1 Q. Because we did not say -- because where does -- is 16:25:59
2 that in the '678 patent, that says the policy 16:26:03
3 describes creating a namespace, or how -- where is the 16:26:07
4 creation of a namespace attached to the policy? I 16:26:14
5 mean, I don't see that connection. 16:26:22

6 A. I see. 16:26:24

7 MR. LU: Objection. Mischaracterizes the 16:26:24
8 testimony. 16:26:25

9 Go ahead. 16:26:27

10 A. I'm saying that in all the embodiments that we see, 16:26:29
11 and my understanding of namespace and what I think a 16:26:34
12 POSITA would understand as creating a namespace, 16:26:37
13 would be influenced by what's in the policy because 16:26:40
14 the way that the namespace is created depends on 16:26:44
15 information in the policy. 16:26:49

16 If you don't have a policy and I say, hey, 16:26:50
17 go create a namespace, you just throw your hands up, 16:26:53
18 like, on what platform? I don't even have a list of 16:26:55
19 cloud platforms here. What encryption am I supposed 16:26:59
20 to use? 16:27:02

21 Because that's part of how you create the 16:27:03
22 namespace. 16:27:05

1 What are the file names supposed to even 16:27:05
2 look like? That's also in the policy. So I don't 16:27:07
3 know how to create a namespace without starting at 16:27:11
4 least with the policy file that answers all those 16:27:14
5 questions that I have. I don't know where to even 16:27:17
6 create a container to start with unless I have the 16:27:19
7 storage information that's in the policy. 16:27:22

8 So I don't think the '678 explicitly says 16:27:27
9 that -- you know, that the policy author is, in 16:27:30
10 essence, influencing how the namespace is created. 16:27:34
11 But I think if you read the patent, it's clear that 16:27:37
12 she writes the policy and that influences the 16:27:39
13 namespace creation because it, at least, tells you 16:27:45
14 where to go to make these containers. 16:27:47

15 Q. Okay. And then you also mention encryption of the 16:27:53
16 chunks by public and private keys. 16:28:08

17 How does encryption of the chunks influence 16:28:13
18 creation of the namespace, if it does at all? 16:28:20

19 A. Because as part of encryption, as we can see in 16:28:25
20 Claim 1, we also decide on the filenames. And the 16:28:28
21 filenames, of course, have to be members of the 16:28:31
22 namespace. 16:28:35

1	Q.	Can you point me where in Claim 1 it says that?	16:28:38
2	A.	Sure.	16:28:44
3		Okay. So Claim 1, the first limitation is,	16:28:57
4		assigning. That's assigning policies to users. And	16:29:00
5		the second one is the encryption of the file, of the	16:29:04
6		content of the file, and it has several steps. And	16:29:08
7		I'm saying that because it's indented below the	16:29:14
8		encrypting limitation.	16:29:16
9		And it says, by: First sub-limitation is,	16:29:19
10		"dividing the file into a plurality of chunks." The	16:29:25
11		second is "creating namespaces for one or more of the	16:29:27
12		plurality of chunks."	16:29:31
13		And then the last one is configuring the	16:29:32
14		namespaces of the one or more chunks to make it	16:29:35
15		searchable.	16:29:39
16		So part of encryption is creating the	16:29:41
17		namespace.	16:29:44
18	Q.	I don't agree with that necessarily, but let's take	16:29:49
19		that as a fact.	16:29:58
20		So how does using a symmetric	16:30:02
21		encryption-key algorithm work to produce -- to create	16:30:08
22		the namespace?	16:30:13

1	MR. LU: Objection. Vague.	16:30:16
2	BY MR. TEHRANCHI:	16:30:18
3	Q. Again, going back to the claim, it says encrypting	16:30:18
4	content of the file. Right?	16:30:23
5	And how does encrypting content of a file	16:30:26
6	with the symmetric encryption key algorithm work to	16:30:35
7	generate -- create the namespace?	16:30:39
8	A. Because --	16:30:45
9	MR. LU: Objection. Vague.	16:30:45
10	A. -- the process of encrypting the file and outputting	16:30:46
11	the file requires that you have a filename, and what	16:30:51
12	part of -- what filenames are possible defines the	16:30:55
13	scope of the namespace, defines what are the possible	16:30:59
14	different filenames that can go in that namespace.	16:31:02
15	I agree with you if you're saying that the	16:31:06
16	contents of the file, if you encrypt that, that's not	16:31:08
17	influencing directly the filename, but these two	16:31:12
18	things go hand in hand in the patent.	16:31:15
19	BY MR. TEHRANCHI:	16:31:24
20	Q. As far as encrypting the contents of the file, it's	16:31:24
21	done on an individual chunk basis; is that correct?	16:31:29
22	A. Yes.	16:31:33

1	Q. Okay. And then the filename, is that the same as the	16:31:33
2	namespace or is that different?	16:31:50
3	MR. LU: Objection. Vague.	16:31:55
4	A. The filename is the name within the namespace. It	16:31:56
5	has to be within the range of acceptable values.	16:32:00
6	BY MR. TEHRANCHI:	16:32:11
7	Q. So can you explain how would a public-key encryption	16:32:29
8	algorithm work when you encrypt individual chunks as	16:32:39
9	it's required by the claim?	16:32:45
10	MR. LU: Objection. Vague. Incomplete	16:32:50
11	hypothetical.	16:33:05
12	A. I'm sorry, are you saying that public-key algorithm	16:33:05
13	is required by the claim?	16:33:08
14	BY MR. TEHRANCHI:	16:33:09
15	Q. So let me -- let me go to your paragraph 71, and in	16:33:10
16	your paragraph 71, you say, "For example, the '678	16:33:13
17	patent teaches that 'each chunk can be encrypted based	16:33:17
18	on public and private/secret keys.'" Right?	16:33:21
19	Do you see that?	16:33:25
20	A. I do, and I'm quoting from the patent there.	16:33:27
21	Q. Right. It's in the patent.	16:33:30
22	So the patent says you can encrypt the	16:33:32

1 chunks based on private or public key algorithms. 16:33:36

2 Now, the claim is not specific about public 16:33:41

3 or private key, but am I correct to assume that the 16:33:45

4 scope of that claim of that encryption of the chunk 16:33:49

5 that is recited in the patents would include public or 16:33:52

6 private key algorithms? 16:33:56

7 A. That would be my reading. 16:34:00

8 Q. Okay. So now my question is, if we're using 16:34:01

9 public-key algorithm, what would be the procedure for 16:34:07

10 generating -- for performing these three steps that 16:34:10

11 you're -- that are under there? 16:34:19

12 MR. LU: Objection. Vague. 16:34:21

13 A. There are multiple ways to do it. Theoretically you 16:34:24

14 could just, as you encrypt the file chunks, apply a 16:34:35

15 public key for which you have the corresponding 16:34:40

16 private key, and -- 16:34:43

17 BY MR. TEHRANCHI: 16:34:47

18 Q. Sorry. Do you as -- which -- can you be more 16:34:48

19 specific? 16:34:51

20 A. Sorry. Sorry. The gateway. The gateway that's 16:34:51

21 performing the encryption would encrypt each of the 16:34:53

22 chunks and then the gateway would presumably have the 16:34:58

1 corresponding decryption key or private key. 16:35:01

2 The patent talks about sometimes the 16:35:06

3 gateway could send keys to the user, so maybe there's 16:35:08

4 times when the private key could be given up to a user 16:35:13

5 under the right circumstances. But obviously, 16:35:15

6 encrypting with a public key, without having the 16:35:19

7 corresponding private key, is a waste of time because 16:35:23

8 you need the decryption key. 16:35:27

9 The only time I can see where you wouldn't 16:35:29

10 need it is if you just want to know if a word exists 16:35:34

11 but you don't need to actually retrieve the file. 16:35:37

12 That sounds kind of silly. 16:35:40

13 So I think -- you know, in the case for a 16:35:41

14 public key, each chunk is encrypted under a public 16:35:44

15 key. And then later on if a keyword is found to be in 16:35:47

16 a file, you could optionally download all the file 16:35:52

17 chunks and then apply the private key that corresponds 16:35:56

18 to that public key to decrypt all of the chunks and 16:36:01

19 reconstitute the file, for example. 16:36:04

20 Q. So the same party would have both the private key and 16:36:08

21 the public key? Or are you saying that the storage 16:36:14

22 provider -- the cloud storage facility or provider has 16:36:17

1	the decryption key which is the private key?	16:36:22
2	MR. LU: Objection. Vague.	16:36:25
3	Mischaracterizes testimony.	16:36:27
4	A. I think it's possible that you could set things up	16:36:31
5	that way. I think it's also possible that you could	16:36:32
6	say, I'm a user and I have my own private key that I	16:36:36
7	don't share with anyone, but I want the gateway to	16:36:42
8	encrypt using my public key all these file chunks,	16:36:45
9	and now the gateway is sort of an innocent third	16:36:48
10	party who can't actually understand anything.	16:36:51
11	But if the gateway asks a query on your	16:36:55
12	behalf and finds that this file contains a keyword and	16:36:58
13	the cloud's providers remit all of these encrypted	16:37:02
14	chunks then the gateway can't understand them, but it	16:37:05
15	could forward it back to you, since you have the	16:37:10
16	private key, and you could undertake the task of	16:37:12
17	decrypting and reconstituting the file yourself.	16:37:16
18	So now different parties could encrypt and	16:37:22
19	decrypt, is what I'm saying. Right? The encryption	16:37:25
20	could be done by the gateway, the decryption by the	16:37:27
21	user, which is one of the beauties of asymmetric	16:37:30
22	cryptography.	16:37:34

1 Q. Wouldn't that be very time-consuming when you're 16:37:41
2 dealing with these chunks? 16:37:44

3 MR. LU: Objection. Vague. 16:37:45

4 A. Certainly if a large file is -- you know, the 16:37:46
5 decryption burden is the heavier burden for 16:37:49
6 public-key cryptography, and so, you know, if the 16:37:53
7 endpoint device didn't have much power maybe that 16:37:57
8 would be undesirable and you would want the gateway 16:37:59
9 to do it, but that's a design -- that's an 16:38:02
10 engineering decision you would want to make. 16:38:05

11 BY MR. TEHRANCHI: 16:38:12

12 Q. In case of a symmetric algorithm, let's say AES, how 16:38:15
13 would this encryption occur, encryption of the chunks 16:38:24
14 between the gateway and the cloud storage facility? 16:38:31

15 A. So in this case now there's only a single key that 16:38:38
16 works to both encrypt and decrypt each chunk, and so 16:38:41
17 anyone who's capable of encrypting the chunk is also 16:38:46
18 capable of decrypting the chunk. And in this case, 16:38:49
19 the gateway would encrypt each chunk using the 16:38:53
20 symmetric key and then deposit the encrypted 16:38:56
21 ciphertext chunk onto a given cloud storage provider. 16:39:01

22 And then if depiction were desired, it 16:39:05

1 would be up to the gateway device or possibly the end 16:39:08
2 user, if it's set up that way, since, as I said, the 16:39:13
3 patent does sometimes talk about giving keys up to 16:39:15
4 the users. The only person in this story who can't 16:39:17
5 decrypt now is the cloud service provider. 16:39:22
6 Q. Okay. All right. We'll get to that point a little 16:39:26
7 bit later. 16:39:36
8 So there are two encryption operations that 16:39:46
9 are ongoing here, as I understand it. Correct me if 16:39:50
10 I'm wrong. You agree that the file chunks are 16:39:57
11 encrypted, and then, although not in Claim 1 16:40:00
12 specifically, but the keywords, the search words, are 16:40:06
13 also encrypted; is that correct? 16:40:11
14 A. In some embodiments, yes, the keyword, the search 16:40:15
15 words can be encrypted as well. 16:40:18
16 Q. Okay. But you are saying that in some embodiments, 16:40:21
17 then, the keywords would need not be encrypted? 16:40:25
18 A. Yeah, I mean, Claim 1 doesn't require that you 16:40:34
19 encrypt keywords. Right? So it just requires that 16:40:36
20 the namespace be configured to facilitate encrypted 16:40:41
21 search. 16:40:45
22 So, for example, maybe you would hash a 16:40:47

1 keyword with a one-way hash to force -- to try and 16:40:49
2 forestall reverse engineering what the key search term 16:40:53
3 was, let's say. That's not encryption. Right? 16:40:56
4 There's no key. But it's another transformation that 16:40:59
5 would serve to obfuscate the search term, and I would 16:41:03
6 think that also would fall under facilitating the 16:41:07
7 search of encrypted data. 16:41:10
8 Q. Okay. So, for example, I don't know, MD5 or whatever 16:41:13
9 hash algorithm, SHA, could be used to produce a hash 16:41:20
10 of the search terms and then that would be used in a 16:41:26
11 query to ask the service provider to -- cloud service 16:41:30
12 provider to provide the chunks; is that correct? 16:41:35
13 MR. LU: Objection. Incomplete 16:41:40
14 hypothetical. 16:41:43
15 A. Certainly that would serve to obscure and hide the 16:41:43
16 search term without using encryption, so that would 16:41:47
17 work. 16:41:52
18 BY MR. TEHRANCHI: 16:41:57
19 Q. Now, there is also an operation here which seems 16:41:57
20 fairly benign, but it says, breaking the files into 16:42:04
21 chunks. 16:42:09
22 Do you need to do that as a part of the 16:42:15

1 encryption of the chunks? 16:42:17

2 MR. LU: Objection. Vague. 16:42:22

3 A. I think in Claim 1 the encrypting limitation starts 16:42:25

4 by saying the first thing you do is to divide the 16:42:34

5 file into chunks. 16:42:36

6 Now, you said you disagreed, so maybe 16:42:37

7 we're reading the claim in a different way, but I 16:42:39

8 read that to mean that the encrypting step of the 16:42:41

9 method claim involves three subsystems, the first of 16:42:46

10 which is dividing the file into chunks. 16:42:51

11 BY MR. TEHRANCHI: 16:42:55

12 Q. Okay. But those chunks are not encrypted yet. 16:42:55

13 Correct? Because I have a little bit of a difficulty 16:42:59

14 understanding what the claim is actually doing, and 16:43:05

15 that's why I'm trying to figure that out. 16:43:08

16 And from the perspective of a person of 16:43:11

17 ordinary skill in the art, and do you agree that a lot 16:43:14

18 of encryption algorithms, they first break up the 16:43:20

19 chunk -- the file into chunks? Is that a fair 16:43:22

20 assessment? 16:43:27

21 MR. LU: Objection. Vague. 16:43:28

22 A. I mean, there are certainly encryption algorithms 16:43:32

1 that start by breaking things into chunks, 16:43:34

2 absolutely. 16:43:37

3 BY MR. TEHRANCHI: 16:43:38

4 Q. Then after you break that up into chunks, then you 16:43:38

5 encrypt it based on whatever algorithm you are using. 16:43:42

6 Correct? 16:43:46

7 A. Yes. 16:43:48

8 Q. Okay. And I think we talked about this a little bit 16:43:51

9 before. What comes out of that encryption of the 16:43:59

10 chunks, it could have a variable length. So, for 16:44:04

11 example, if your chunk has size A, the encrypted chunk 16:44:10

12 could have size B, and another chunk with size A could 16:44:16

13 have a length of size C; is that correct? 16:44:22

14 MR. LU: Objection. Incomplete 16:44:31

15 hypothetical. 16:44:36

16 A. I'm trying to think of any encryption systems that do 16:44:36

17 that. Usually -- it's very common that length of 16:44:40

18 size A could come out as ciphertext larger than A; 16:44:45

19 like, it grows. And we saw an example in the patent 16:44:50

20 itself, in fact, where "Ronn" became six letters. 16:44:53

21 I don't know that I can think of a system 16:45:00

22 where you encrypt the same chunk twice and you get one 16:45:02

1 ciphertext longer than the other. Usually it expands 16:45:07
2 by a fixed amount at each time because you're adding, 16:45:11
3 like, a certain number of random bits into the 16:45:16
4 plaintext. Maybe there's a system where it grows by 16:45:19
5 variable amounts each time you encrypt the same thing, 16:45:23
6 I just can't think of one. 16:45:26

7 There are also systems, and I have a -- I 16:45:30
8 sort of created this area, in fact, where you keep the 16:45:31
9 domain and the ciphertext range the same so they don't 16:45:37
10 grow, they fit into the same space, even after it's 16:45:39
11 encrypted. 16:45:45

12 Q. Okay. Now, in terms of the actual values that are 16:45:45
13 produced, if you encrypt the same chunk twice, would 16:45:52
14 you get the same ciphertext in both cases or could 16:46:00
15 they be different? 16:46:03

16 MR. LU: Objection. Incomplete 16:46:06
17 hypothetical. 16:46:08

18 A. It depends on the algorithm. Some algorithms produce 16:46:08
19 the same thing every time. We try not to do that, 16:46:12
20 for reasons I could get into if you're interested. 16:46:17
21 But another set of algorithms could add randomness, 16:46:19
22 so that even if you encrypt the same thing twice, you 16:46:25

1 get two different outputs. Because that way I could 16:46:28
2 show you two cybertexts and you can't tell it's the 16:46:33
3 same plaintext because they're different, and that's 16:46:36
4 a good thing. 16:46:38

5 BY MR. TEHRANCHI: 16:46:43

6 Q. And up to this point we were talking about, really, 16:46:43
7 encrypting the chunks. Now, we also talked about 16:46:46
8 encrypting the search words. 16:46:50

9 Could the same thing be applied to 16:46:53
10 encrypting the search words so that it produces 16:46:55
11 different search query encrypted values for the same 16:47:02
12 search term? 16:47:08

13 MR. LU: Objection. Vague. 16:47:10

14 A. There, that would be highly undesirable. In fact, it 16:47:12
15 might render the system inoperable because you need 16:47:17
16 to have the same ciphertext to search for, that was 16:47:22
17 generated when you first set that term as -- into the 16:47:27
18 index. Obviously if you got a separate ciphertext, 16:47:31
19 you wouldn't get a match anymore. 16:47:35

20 So, there, if you're using encryption, you 16:47:37
21 need to use deterministic encryption that always 16:47:39
22 produces the same output. 16:47:43

1 Of course, if you use the hash function, 16:47:44
2 you're all -- you're good to go because they always 16:47:47
3 produce the same output for the same input. 16:47:49

4 Q. And also wouldn't one benefit of the hash function be 16:47:56
5 that it reduces -- could potentially reduce the size? 16:48:00

6 Usually hashes are smaller in size than the 16:48:06
7 plaintext that you're trying to hash. Is that a 16:48:09
8 reasonable statement? 16:48:13

9 A. Hash functions typically shrink a large file down to 16:48:19
10 a small size. But for search terms -- you know, so 16:48:25
11 let's take, like, you -- I think you mentioned SHA-1. 16:48:29
12 SHA-1 is 160 bits output, so that's 20 characters, if 16:48:34
13 you were to put them into 8-bit character chunks. 16:48:41

14 A lot of search terms might be shorter 16:48:45
15 than 20 characters, and so SHA-1 might actually 16:48:48
16 expand search words since they're relatively small. 16:48:51
17 But certainly if you took a big file and you turned 16:48:54
18 that into 20 characters, that's going to comprise -- 16:48:59
19 that's going to constitute a shrinking. 16:49:02

20 Q. Okay. Fair enough, then. 16:49:04

21 So let's maybe just switch back a little 16:49:19
22 bit to the namespace. I'm still a little bit unclear 16:49:23

1	about creating the namespace.	16:49:26
2	So when you create the namespace in the	16:49:29
3	context of the '678 patent, are you required to	16:49:32
4	identify all the possible values for the name range --	16:49:37
5	[Simultaneous speaking]	16:49:48
6	MR. LU: Objection. Objection. Vague.	16:49:48
7	STENOGRAPHER: Can you just repeat the end	16:49:58
8	of that? "...for the name range"...	16:49:59
9	BY MR. TEHRANCHI:	16:50:01
10	Q. So are you required to identify all the possible	16:50:01
11	values in that namespace?	16:50:08
12	A. Yes and no. So you have to indicate the set of	16:50:12
13	values or set of names via some kind of constraint or	16:50:19
14	description. It could be something that allows you	16:50:24
15	to see all the values. Obviously if I said numbers	16:50:28
16	between 1 and 1 million, you know what that means, I	16:50:33
17	know what that means, and if I wrote down a number	16:50:38
18	you could say that it's within the range or that's	16:50:41
19	not within the range just because your brain is able	16:50:43
20	to value a number and tell me whether it's in a	16:50:47
21	range.	16:50:50
22	But if I say that the namespace is all	16:50:51

1 possible outputs from SHA-1, you understand what that 16:50:57
2 means. But if I give you 160 bits and I say, is this 16:51:05
3 in the namespace, we may not be able to know because 16:51:08
4 we can't reverse SHA-1. Right? 16:51:10

5 So I can say the namespace is all possible 16:51:15
6 outputs of the algorithm even though I can't enumerate 16:51:17
7 all possible outputs because nobody knows what all 16:51:19
8 possible outputs are, nor can I tell you for a given 16:51:23
9 160-bit string whether SHA could actually output that 16:51:28
10 ever, unless I secretly know the input that did it. 16:51:31
11 But if I gave it to you without telling you what the 16:51:34
12 input was, you would have no idea typically without 16:51:38
13 breaking SHA-1 somehow. 16:51:41

14 Q. So back to breaking -- producing this searchable 16:51:45
15 encrypted file, does the claim or the patent limit the 16:52:13
16 file to a text file? 16:52:20

17 MR. LU: Objection. Vague. 16:52:26

18 BY MR. TEHRANCHI: 16:52:37

19 Q. Let me rephrase. I think it's clear, but... 16:52:37

20 So if you have a text file, you can produce 16:52:40
21 a searchable encrypted file based on the claims and 16:52:43
22 the algorithms or a description that is described in 16:52:47

1	'678. Do you agree with that?	16:52:49
2	A. If you have a text file, yes, you can.	16:52:54
3	Q. Can you do that the same -- can you apply the same	16:52:56
4	technique that's described and claimed in '678 to an	16:53:01
5	audio file?	16:53:04
6	MR. Objection. Vague.	16:53:08
7	A. So I -- audio files, depending on the format, could	16:53:15
8	have metadata or tags that maybe could be searchable.	16:53:20
9	But for the most part, I don't know that, you know,	16:53:26
10	there are analogs to keywords to search an audio file	16:53:40
11	for, say, an example, sound. Right?	16:53:47
12	So if you had a beep in an audio file and	16:53:52
13	you wanted to be able to search for any instances of	16:53:56
14	that beep, maybe you could do that. I was thinking of	16:53:59
15	it in terms of keywords searched for in PDFs or Word	16:54:07
16	or text or things like this. I don't know how that	16:54:10
17	would look for other kinds of data, for movies or	16:54:15
18	sound data.	16:54:19
19	This is something I would have to think	16:54:22
20	about whether it makes sense. I don't recall that the	16:54:24
21	'678 ever says, text files are the only thing that	16:54:27
22	we're covering here. It just says, searchable	16:54:32

1	encryption. So it would take me some time. I would	16:54:34
2	have to go figure out whether it makes sense for an	16:54:38
3	audio file to do this.	16:54:40
4	Q. That's fair enough.	16:54:44
5	So you haven't thought about that and you	16:54:47
6	are not in a position to answer whether audio files	16:54:51
7	can be subject to this kind of searchable encryption	16:54:54
8	methodology.	16:55:00
9	A. Yeah, I was really trying to respond to the petition	16:55:03
10	and petitioner's expert, and I didn't see that raised	16:55:06
11	anywhere so I didn't really spend time thinking	16:55:10
12	about -- it's an interesting question, for sure, and	16:55:12
13	you maybe know more than I do given the watermarking	16:55:14
14	work you've done, but I, sitting here, couldn't	16:55:17
15	answer.	16:55:20
16	Q. Are you familiar with Shazam technologies?	16:55:20
17	A. Only to the first approximation. I don't know --	16:55:27
18	Q. Okay. It's -- it's probably beyond the scope of --	16:55:29
19	Shazam is, but I think it's a fair question to ask if	16:55:35
20	these claims are or this terminology -- you know, that	16:55:39
21	files are limited to just text files or if they could	16:55:42
22	include audio files, video files, image files, other	16:55:46

1	known text.	16:55:52
2	A. I mean, I like the question, it's interesting and I'd	16:55:54
3	love to think about it, but I don't have a ready	16:55:57
4	answer. I just -- all I can say is, I don't recall a	16:55:59
5	disavowal of non-text files anywhere in the patent.	16:56:02
6	Q. Okay. Fair enough.	16:56:09
7	So in your declaration -- and I forgot	16:56:37
8	where it was exactly, but it's not relevant to this	16:56:41
9	question -- you mentioned actually during the	16:56:45
10	deposition about Appendix A part of this.	16:56:48
11	Are you familiar with that paper in	16:56:52
12	Appendix A of Exhibit 1001?	16:56:55
13	A. I'm familiar to some extent. I read it, but it's	16:57:00
14	been a while. I just remember that I -- I said the	16:57:04
15	word "Dragonfruit" because I remember that was the	16:57:07
16	name of their system that they created.	16:57:09
17	Q. Okay. So I'd like to go through that a little bit	16:57:11
18	with you. Maybe we'll start and then we can -- okay,	16:57:17
19	I don't think it's going to be that long, but could	16:57:27
20	you go to Appendix A in 1001.	16:57:29
21	A. I'm there.	16:57:35
22	Q. Okay. So if you go to page -- end of page 26 of 30,	16:57:37

1 and beginning of page 27 of 30 in that appendix. The 16:57:58
2 page numbers are on the bottom. 16:58:06
3 A. I see them. 16:58:12
4 Q. There is a section, Section IV, Roman Numeral IV, that 16:58:13
5 says, "Encoding Searchable Indices." 16:58:17
6 Do you see that? 16:58:19
7 A. I see that heading, yes. 16:58:21
8 Q. Okay. So in that section -- and feel free to kind of 16:58:23
9 review that if you don't remember -- it does talk 16:58:35
10 about four different steps, and that's in the left 16:58:39
11 column on page 27. One of them is Setup, one of them 16:58:49
12 is Encryption, one of them is Token, and the fourth 16:58:53
13 one is Query. 16:58:58
14 Do you see that? 16:59:02
15 A. I do see those four headings. 16:59:04
16 Q. Okay. In Query, the last one, says, This is the final 16:59:06
17 step of searchable encryption scheme -- oh, the -- 16:59:17
18 sorry. "The final step of the searchable encryption 16:59:21
19 scheme is processing the received query by the cloud 16:59:24
20 provider that has access to the encrypted records, and 16:59:30
21 the single private key that the trusted gateway has 16:59:34
22 sent." 16:59:36

1 So maybe it's not fair for me to just point 16:59:37
2 to that, to that last query step. 16:59:40

3 Do you want to take some time on this, 16:59:47
4 you're already familiar with it, to kind of read 16:59:50
5 through the prior three steps so when we talk about 16:59:53
6 step four we're all on the same page? 16:59:55

7 A. Sure. Yeah. 17:00:00

8 Okay, I read through all of it. 17:03:55

9 Q. Okay. So back to the Query section, it seems to 17:03:57
10 explain that there are at least two variations, and in 17:04:07
11 one case the cloud provider will retrieve and 17:04:10
12 correctly decrypt only the records which match the 17:04:17
13 received query. 17:04:21

14 And in that case, the cloud provider needs 17:04:23
15 to have that secret key to be able to do that; is that 17:04:26
16 correct? 17:04:29

17 A. I'm not sure. So why -- where are you seeing that 17:04:34
18 there are two variant -- two variants? 17:04:37

19 Q. So that's one variant. And then -- well, let's start 17:04:41
20 with that one. 17:04:43

21 Is that the correct interpretation, that 17:04:44
22 the cloud provider in that scenario would have the 17:04:46

1	secret key and is able to decrypt and -- retrieve and	17:04:51
2	correctly decrypt only the records that match the	17:04:57
3	received query?	17:05:00
4	A. Right.	17:05:06
5	MR. LU: Objection. Vague.	17:05:06
6	A. It says that, but I don't see that it says that there	17:05:07
7	are variants of it. I think that is --	17:05:09
8	BY MR. TEHRANCHI:	17:05:11
9	Q. Okay. I'll get to the -- I'll get to the variant in a	17:05:11
10	minute, but I think that's -- let's agree or disagree,	17:05:14
11	that is one explained in the Query section. Okay?	17:05:17
12	A. Okay.	17:05:25
13	Q. And then if you move to the last sentence, is it -- it	17:05:28
14	says, "It is important to mention that for absolute	17:05:32
15	data disclosure prevention, the trusted gateway should	17:05:34
16	encrypt the records using a symmetric key and unique	17:05:38
17	salt such that R is already encrypted and the cloud	17:05:41
18	provider is not allowed to see the actual record."	17:05:45
19	Do you characterize that as a second	17:05:48
20	variation where the cloud provider is not able at all	17:05:54
21	to see the record -- decrypt the record and see it?	17:05:57
22	MR. LU: Objection. Vague.	17:06:01

1 A. I, once again, didn't read it as a variation and I 17:06:02
2 don't see it where it says that absolute data 17:06:07
3 disclosure prevention is optional, which I think you 17:06:12
4 are inferring, the way you're reading it. 17:06:14

5 You seem to be thinking, like, and then 17:06:17
6 there's this optional feature that you can turn on or 17:06:20
7 off that creates a second variant of the scheme. But 17:06:24
8 the way I read it, at least, was it's important to 17:06:27
9 mention that you need this additional thing to not 17:06:31
10 forget that the record R has to already be encrypted 17:06:33
11 before it's -- before it's encrypted again with the 17:06:38
12 public key. 17:06:41

13 Q. So how do you account for the prior sentence that 17:06:48
14 says -- well, the prior sentence, the sentence that 17:06:53
15 says, "It is easy to follow that the cloud provider 17:06:55
16 will retrieve and correctly decrypt only the records 17:07:01
17 which match the received query, and will get 0 as a 17:07:05
18 result of all other decryptions"? 17:07:08

19 A. Right. So what it's saying is that the cloud 17:07:13
20 provider will be provided with a private key and they 17:07:19
21 will apply it to these records and only matched 17:07:22
22 records will return a non-zero result -- that's still 17:07:28

1 ciphertext, according to what's later in that
2 paragraph -- or they'll get zero, meaning, this is
3 irrelevant, don't send this back to the user because
4 it's -- there's no -- this is a record-by-record
5 search. Right? This is not a -- this is not an
6 entire file search.

17:07:33

17:07:35

17:07:40

17:07:44

17:07:46

17:07:49

7 In other words, I'm not saying, if this
8 keyword occurs anywhere in this file, send me the
9 entire file. They're trying to add another feature on
10 top of that, as they describe on page 26. The last
11 sentence on page 26, "As a result, the whole dataset
12 must be returned for any query, even if the user is
13 only interested in records with a certain property."

17:07:51

17:07:54

17:07:57

17:08:00

17:08:06

17:08:09

17:08:12

14 So they're trying to make it so their
15 system can return only the records that are relevant
16 for the query and not the entire file. And so the
17 feature that they have added is, okay, well, I'll give
18 you this key and you'll either get ciphertext, which I
19 do want because there's a hit in that record, or
20 you'll get zero, which means there's no match in that
21 record, don't send me that part.

17:08:14

17:08:17

17:08:21

17:08:25

17:08:29

17:08:32

17:08:35

17:08:38

22 But in neither case does the cloud provider

17:08:39

1 learn the actual contents of the record because 17:08:43
2 there's a second decryption that has to occur. 17:08:45

3 The cloud provider does learn how many hits 17:08:50
4 there were for the term, I suppose you can't hide that 17:08:53
5 because you're allowing this record-by-record 17:08:55
6 searching, but they don't actually see the record. 17:08:57

7 Q. So when it says that the cloud provider will retrieve 17:09:01
8 and correctly decrypt only the records which match the 17:09:06
9 received query, that doesn't mean that those records 17:09:12
10 that are correctly decrypted are plaintext. Is that 17:09:17
11 your opinion? 17:09:22

12 A. The way I read this paragraph, it's not. There's a 17:09:24
13 second decryption that has to occur at the gateway, 17:09:28
14 according to what's in the last part of that 17:09:31
15 paragraph. 17:09:32

16 Q. So you're saying that the last sentence in that 17:09:33
17 paragraph is a requirement; you cannot -- this would 17:09:46
18 not work or it would not -- you know, the -- okay. 17:09:49
19 Scratch that. 17:09:53

20 The reason I'm asking this is because, to 17:09:54
21 me, it seems -- and you can disagree with me and let 17:09:57
22 me know your opinion on this -- is that it is 17:10:01

1 important to mention that, for absolute data 17:10:04
2 disclosure prevention you need to do what comes for 17:10:07
3 that -- for the rest of that sentence. 17:10:12

4 And up to that point, there were no 17:10:15
5 explanation that you actually need not to share things 17:10:19
6 with the cloud provider. 17:10:24

7 So, again, the question is that, do you 17:10:28
8 think that the first sentence in here requires 17:10:32
9 encryption of the record so you get the ciphertext or 17:10:45
10 you would not get the ciphertext -- sorry, the 17:10:48
11 plaintext, or is it the case that you would never get 17:10:52
12 the plaintext with this technique? 17:10:58

13 A. I mean, I'll caveat this by saying, you know, I read 17:11:04
14 this section just now. I read it probably a month or 17:11:10
15 two ago as well. But reading it just now, I can't 17:11:14
16 attest with absolute certainty as to how the system 17:11:18
17 works. But when you asked me to read this paragraph, 17:11:23
18 I read that last sentence, it is important to mention 17:11:26
19 that XYZ must happen. I didn't read it as, it's 17:11:31
20 important -- it's important to mention that you -- 17:11:35
21 there's some stuff you might want to do. 17:11:38

22 So I think of it as a requirement. I think 17:11:41

1 that the cloud provider only gets ciphertext or zero, 17:11:44
2 never gets plaintext. It would seem silly to me to 17:11:48
3 have an encrypted storage system and then give up the 17:11:52
4 keys to the cloud provider. It's like, why did you 17:11:56
5 bother encrypting things in the first place then? 17:11:59
6 Q. Okay. Fair enough. That answers my question. 17:12:03
7 Let's move a little bit further in this 17:12:10
8 document. 17:12:13
9 THE WITNESS: Mr. Tehranchi, is this okay 17:12:14
10 time for a break? We're at a little over an hour in. 17:12:16
11 MR. TEHRANCHI: Yes, yes. Let's do 3:30 17:12:19
12 your time. Would that work? 17:12:27
13 THE WITNESS: Perfect. I'll see you then. 17:12:29
14 MR. TEHRANCHI: Thank you. 17:12:31
15 THE WITNESS: Thanks so much. 17:12:32
16 (Off the record at 5:12 p.m.) 17:12:33
17 (Back on the record at 5:31 p.m.) 17:31:46
18 BY MR. TEHRANCHI: 17:31:51
19 Q. Dr. Black, let's continue with Appendix A of 17:31:52
20 Exhibit 1001, and let's move to Section V on page 28. 17:32:01
21 A. Okay. I'm there. 17:32:12
22 Q. Okay. The third full paragraph under Section V talks 17:32:13

1	about a possible boolean search text that says Race =	17:32:29
2	Asian and age greater than 35.	17:32:34
3	Do you see that?	17:32:37
4	A. I do.	17:32:38
5	Q. Okay. And you can spend sometime reading that	17:32:43
6	paragraph or this section, but my question is about	17:32:45
7	that specific example for the search terms.	17:32:48
8	A. Okay. Well, maybe you want to ask your question and	17:32:58
9	then if I need to read more to understand, I might	17:33:00
10	ask for a minute.	17:33:03
11	Q. Okay. So let's discard the second part of that query,	17:33:04
12	the age prong. Let's look at just the race.	17:33:09
13	So when the query says, Race = Asian, what	17:33:12
14	is your understanding of how the index is produced?	17:33:17
15	And let me be a little bit more specific and you can	17:33:24
16	elaborate on that.	17:33:28
17	So does it mean that, let's say, this is a	17:33:29
18	text document, it must specifically say "Asian" in the	17:33:33
19	text, or does it mean if the text says, for example,	17:33:40
20	"Filipino man," would that also show up as part of the	17:33:45
21	search query?	17:33:50
22	MR. LU: Objection. Vague.	17:33:54

1 Mischaracterizes the document. Incomplete 17:33:54
2 hypothetical. 17:33:54
3 A. So, again, with the caveat that I haven't read the 17:34:25
4 entire paper recently and I'm not sure of the details 17:34:28
5 of its implementation, it seems to be saying that 17:34:30
6 it's doing queries on tables and tables that are 17:34:36
7 comprised of records because it even says in that 17:34:40
8 sentence you read, it wants to see all records where 17:34:44
9 these two boolean conditions both appear or occur. 17:34:47
10 How those records are encoded is really up 17:34:52
11 for grabs. I used to work in a database company, and 17:35:00
12 so, you know, we encode records in our tables all 17:35:05
13 kinds of different ways. So I don't know that the 17:35:09
14 text A-s-i-a-n necessarily need appear for this query 17:35:12
15 to be satisfied. Race is probably a column in the 17:35:21
16 table, it's typical, so you're going to search down 17:35:24
17 the columns to look for a match. 17:35:27
18 If "Asian" were in quotes then I would 17:35:29
19 maybe hazard a guess that they're looking for the 17:35:33
20 literal word A-s-i-a-n. But since it's not, I don't 17:35:35
21 know if that means it's just a categorization or a 17:35:43
22 designation or a number. So I guess that's a 17:35:45

1	longwinded way of saying I'm not sure what the answer	17:35:49
2	is to your question.	17:35:51
3	Q. Okay. That's fair enough.	17:35:54
4	But it -- is your answer, then, that it	17:35:55
5	could be done in different ways, the Asian could	17:35:57
6	appear verbatim in the document or it could be an	17:36:02
7	interpretation of, in the example that I said,	17:36:06
8	"Filipino man," that could in some implementations be	17:36:10
9	tagged or produce a positive query result?	17:36:17
10	MR. LU: Objection. Vague. Incomplete	17:36:21
11	hypothetical.	17:36:25
12	A. Yeah, for something that literally says "Filipino	17:36:25
13	man," for it to be -- turn up as a search result for	17:36:28
14	Asian, there would have to be some kind of indication	17:36:31
15	that classifies that as an Asian person. You	17:36:33
16	wouldn't get obviously a verbatim match between the	17:36:39
17	word "Asian" and the two words, "Filipino man."	17:36:43
18	BY MR. TEHRANCHI:	17:36:46
19	Q. Okay. But my question is, is the search methodology	17:36:46
20	limited to verbatim searching for words? And I	17:36:51
21	believe you said that's not the case, but I just want	17:36:56
22	to confirm that your answer is that it doesn't have to	17:36:58

1 be a verbatim search for that word. 17:37:01

2 MR. LU: Objection. Vague. 17:37:07

3 A. In this exact system, Dragonfruit, I don't know. 17:37:09

4 Depends on how they implemented it. But I'm saying 17:37:13

5 that it -- as a database professional, this would 17:37:15

6 have been implemented in many different ways, not 17:37:21

7 solely by writing the word down literally. 17:37:23

8 BY MR. TEHRANCHI: 17:37:26

9 Q. Okay. Fair enough. 17:37:26

10 Let's move to the second prong, the age 17:37:28

11 part of this. Obviously it says "age" and a greater 17:37:30

12 sign. Is it fair to say this is similar to the age -- 17:37:37

13 the race query where the words "greater than 35" need 17:37:43

14 not appear verbatim in the document? 17:37:48

15 A. Correct. At least in my experience. I don't know 17:37:54

16 about the specific system. 17:37:59

17 Q. Okay. And then in terms of -- these are search terms. 17:38:00

18 So when this is sent to the cloud storage facility or 17:38:07

19 provider, is -- are these terms individually encrypted 17:38:14

20 or is the search query with "and" all of that is 17:38:20

21 encrypted? 17:38:27

22 A. It doesn't say in the paragraph that I'm looking at, 17:38:31

1 that you directed me to. It might be somewhere in 17:38:55
2 this paper, but I don't recall how they handle those 17:38:58
3 compound queries or if it's described here. So I 17:39:02
4 would have to go and study the paper to really know 17:39:05
5 the answer, if it's even in here. 17:39:07

6 Q. Okay. So let's -- you know, obviously this paper is 17:39:09
7 an appendix to the patent itself, so it is part of the 17:39:12
8 patent, and so let's kind of generalize about the 17:39:16
9 claims. 17:39:20

10 In your view, are the claims -- well, I 17:39:24
11 don't think the Claim 1 actually requires encryption 17:39:28
12 of the query words. But in the system -- let's move 17:39:31
13 to the '678 patent in general. And you've said in 17:39:38
14 your declaration that these search words or keywords 17:39:42
15 are encrypted. 17:39:47

16 Do you need to encrypt each search term 17:39:48
17 separately? Do you need to encrypt to multiple search 17:39:54
18 words, search keywords together, or it doesn't matter, 17:40:02
19 you could do either way? 17:40:06

20 MR. LU: Hold on. Objection to the extent 17:40:10
21 it mischaracterizes the law regarding incorporation by 17:40:12
22 reference within a prior art reference or within a 17:40:15

1 patent. And objection to the form of the question. 17:40:19

2 A. So I believe your question was if you want to do a 17:40:26

3 search on two words? Maybe you should reask it. I 17:40:34

4 think I lost the thread here. 17:40:39

5 BY MR. TEHRANCHI: 17:40:41

6 Q. Yes. So let's go back to that example of two search 17:40:41

7 terms with race and with age. 17:40:44

8 If those are -- if you want to search the 17:40:48

9 cloud storage provider's database or facility, do you 17:40:52

10 have to separately encrypt those search terms? Do you 17:40:58

11 have to encrypt them together? Or you could do either 17:41:03

12 way, the patent is not specific? 17:41:07

13 A. I mean, for Claim 1, the patent just says that you 17:41:14

14 configure the namespaces such that the content of the 17:41:17

15 file is encrypted in a way that's searchable. That's 17:41:20

16 it. 17:41:25

17 Now, the encryption of the keywords that 17:41:26

18 you said is in my declaration, I'm talking about some 17:41:29

19 embodiments in which they give more details on how you 17:41:33

20 might implement this. And, there, you select what 17:41:37

21 keywords you anticipate will be searched for in the 17:41:41

22 future, and if you only anticipate, you know, "red" 17:41:44

1 and "car," and then those are placed as encrypted 17:41:52
2 keywords, let's say, in the filenames, and then you 17:41:56
3 want to do "red car" together as a single term, if you 17:42:01
4 didn't preselect that as a keyword, you can't search 17:42:07
5 for it now. 17:42:10

6 You could search for each word individually 17:42:10
7 and say, does the word "red" and the word "car," do 17:42:13
8 both of those appear in some file. You could answer 17:42:17
9 that question. But you couldn't answer the question, 17:42:20
10 does it appear red, space, car as a phrase because you 17:42:23
11 didn't use that as a keyword. 17:42:28

12 So anything that wasn't a keyword wouldn't 17:42:29
13 be searchable unless you thought of that in advance or 17:42:32
14 added it later. 17:42:38

15 Q. Can you do the searching sequentially? So search for 17:42:47
16 race Asian first and get some results, and then age 17:42:54
17 greater than 35 and get additional results? 17:42:58

18 A. If we're going out to the Dragonfruit example where 17:43:08
19 they're actually returning records. Right? So 17:43:13
20 you're not returning the entire file, you're 17:43:16
21 returning portions of a file, records within a file. 17:43:20
22 You could just say race equals Asian, and then if 17:43:23

1 those results were returned, you could then yourself 17:43:28
2 look for age greater than 35 among the search results 17:43:32
3 you got. 17:43:36

4 I don't think it would be very efficient to 17:43:37
5 do race equals Asian and then get a bunch of 17:43:40
6 ciphertext, and then Asian greater than 35 and get a 17:43:44
7 bunch more ciphertext, and then try to match them up 17:43:49
8 before decrypting. I suppose that would work, I just 17:43:52
9 don't think it would make much sense. 17:43:55

10 Q. I guess what I'm trying to find out is, in that 17:43:56
11 specific example where they have two search terms 17:43:59
12 clearly, and it's an "and" between them, are you 17:44:03
13 saying that the two together could have -- they have 17:44:09
14 to be encrypted? 17:44:13

15 Because they are actually conducting that 17:44:15
16 search, so -- and they're getting results. So I just 17:44:17
17 want to understand how that encryption takes place for 17:44:20
18 the search word. 17:44:27

19 MR. LU: Objection. Vague. Incomplete 17:44:28
20 hypothetical. 17:44:31

21 A. Yeah, there are several ways to do it, and I don't 17:44:31
22 know how, in the instance that we're talking about in 17:44:36

1 Dragonfruit, that's performed, whether it's -- I 17:44:39
2 think this goes to your question whether the whole 17:44:43
3 meatball is encrypted at once and then sent or if 17:44:45
4 they are doing each part individually and then 17:44:49
5 implementing the ampersand, the "and" boolean 17:44:51
6 operator after the search. I think you have some 17:44:57
7 options there and I don't know that the paper 17:45:00
8 necessarily tells us how they're doing it. 17:45:01
9 Q. Okay. That's fair enough. Let's move to 17:45:05
10 paragraph 143 of your declaration. 17:45:26
11 A. Okay. 17:45:39
12 Q. And here, you -- in paragraph 143 -- yeah, please read 17:45:39
13 that, so I'll ask the question. It's a short enough 17:45:48
14 paragraph that it shouldn't take you very long. 17:45:54
15 A. Okay, I read it. 17:46:10
16 Q. Okay. So -- and we can go to Claim 1, if you don't 17:46:11
17 remember it, but Claim 1 actually says -- let me read 17:46:15
18 it so I'm not misstating what it says. 17:46:24
19 So it says, "encrypting, by the gateway 17:46:29
20 device, using cryptographic key information defined by 17:46:39
21 the policy..." 17:46:43
22 So the questions here are about the 17:46:47

1 cryptographic key information that are defined by the 17:46:50
2 policy. 17:46:53

3 In paragraph 143, the last sentence, you 17:46:56
4 say that, "A POSITA would therefore understand that 17:46:59
5 'cryptographic key information' at least includes 17:47:02
6 defining the encryption and/or decryption keys and 17:47:06
7 encryption type." 17:47:11

8 Do you see that? 17:47:12

9 A. I do. 17:47:15

10 Q. Okay. So does that mean cryptographic key information 17:47:15
11 must include two things, at least two things, 17:47:22
12 encryption or decryption keys, and encryption type? 17:47:30

13 MR. LU: Objection. Mischaracterizes the 17:47:36
14 document. 17:47:37

15 BY MR. TEHRANCHI: 17:47:46

16 Q. Dr. Black, you tell me what it must include in that -- 17:47:46
17 in the cryptographic key information, how many items. 17:47:50

18 MR. LU: Objection. Form. 17:47:55

19 A. So my declaration 143, paragraph 143, I say, "A 17:48:16
20 POSITA would therefore understand that 'cryptographic 17:48:22
21 key information' at least includes defining the 17:48:25
22 encryption and/or decryption keys and encryption 17:48:31

1	type."	17:48:34
2	But I think "defining" doesn't necessarily	17:48:35
3	mean containing. So I would think that you could	17:48:40
4	define a key by just saying this is the key and	17:48:45
5	giving a pointer to it. I don't think you	17:48:49
6	necessarily have to hold the key.	17:48:51
7	But I think you have to have some	17:48:53
8	definition. At least that would be my read of	17:48:55
9	"cryptographic key information," the term from	17:48:58
10	Claim 1.	17:49:02
11	BY MR. TEHRANCHI:	17:49:05
12	Q. Okay. And do you have to also include encryption	17:49:06
13	type?	17:49:11
14	Let me first -- scratch that before you	17:49:11
15	answer that.	17:49:15
16	What do you mean by "encryption type"?	17:49:16
17	A. The item of encryption. In other words, whether I'm	17:49:24
18	doing symmetric or asymmetric, and probably the	17:49:28
19	algorithm that's being used. These are typical	17:49:32
20	things that, you know, if you connect to Amazon, you	17:49:37
21	get that information back in a certificate. It tells	17:49:40
22	you the encryption type that's being used as part of	17:49:44

1	the key information.	17:49:47
2	BY MR. TEHRANCHI:	17:49:55
3	Q. So if it -- if it -- if the cryptographic key	17:49:56
4	information does not specify or does not define	17:49:59
5	encryption type, that's outside of the scope of	17:50:04
6	information defined -- of the cryptographic key	17:50:13
7	information defined by the policy; is that right?	17:50:16
8	MR. LU: Objection. Mischaracterizes the	17:50:20
9	document.	17:50:22
10	A. So the claim language is using "cryptographic key	17:50:44
11	information" defined by the policy. And then in my	17:50:47
12	declaration, a quote from an embodiment, it says	17:50:52
13	that -- let me actually read what the patent actually	17:51:02
14	says.	17:51:04
15	In implementation. This is the top of	17:51:08
16	column 4. So it does say, "According to one	17:51:21
17	embodiment" -- "selected policy can be used to define	17:51:24
18	encryption keys, decryption keys, and encryption type,	17:51:29
19	among other attributes when carrying out the	17:51:33
20	encryption of data."	17:51:35
21	And I think what we're -- what you're	17:51:39
22	asking me is what must be contained in this claim term	17:51:41

1 "key information." Right? What are the minimum 17:51:48
2 requirements that have to be in cryptographic key 17:51:52
3 information. 17:51:55
4 Q. That's right. Based on your statement here. 17:51:56
5 And, actually, you may have pointed to 17:51:58
6 the -- you know, and may have answered it already in 17:52:01
7 column 4, that you said, this is in one embodiment. 17:52:05
8 So a -- please answer that question and then I'll have 17:52:09
9 a followup regarding the embodiment. 17:52:13
10 MR. LU: Counsel, can you -- what's the 17:52:19
11 pending question? 17:52:20
12 BY MR. TEHRANCHI: 17:52:21
13 Q. The pending question is, based on the last sentence in 17:52:21
14 paragraph 143, what must be included as part of 17:52:24
15 cryptographic key information? 17:52:31
16 MR. LU: Objection. Mischaracterizes the 17:52:38
17 document. 17:52:39
18 A. I would say that the -- I mean, the cryptographic key 17:53:11
19 information in the policy must have information that 17:53:15
20 describes something about the key. It could be the 17:53:20
21 key itself, it could be where to find the key, it 17:53:25
22 could be the length of the key, it could be the 17:53:28

1	encryption type, but it has to have information about	17:53:31
2	the key. I mean, it's in the name itself obviously.	17:53:36
3	BY MR. TEHRANCHI:	17:53:40
4	Q. Yeah, that's -- that's fair enough. I think that the	17:53:50
5	record is clear based on what you have here, but, you	17:53:55
6	know, my question is about the "and" in that sentence,	17:54:00
7	the last "and" that says, "and encryption type."	17:54:05
8	To me, that conveys that you must define	17:54:09
9	encryption type as part of cryptographic key	17:54:15
10	information. Am I correct or am I reading that	17:54:22
11	sentence wrong?	17:54:25
12	MR. LU: Objection. Mischaracterizes the	17:54:30
13	document.	17:54:31
14	A. I think I should have been clearer when I wrote this	17:54:32
15	and said, you know, in this embodiment a POSITA would	17:54:34
16	have understood that the key information has at least	17:54:38
17	these constituent parts. But I wouldn't say that, in	17:54:41
18	every case, cryptographic key information must have	17:54:47
19	encryption and/or decryption keys defined and	17:54:53
20	encryption type in order to meet the claim term.	17:54:56
21	BY MR. TEHRANCHI:	17:55:02
22	Q. That's fair enough. Thank you.	17:55:03

1	MR. TEHRANCHI: I don't have anymore	17:55:20
2	questions.	17:55:21
3	So, Counsel, do you have any redirect?	17:55:22
4	MR. LU: Sure, I have one short question.	17:55:30
5	EXAMINATION	17:55:30
6	BY MR. LU:	17:55:30
7	Q. So looking at the same paragraph 143, is it possible	17:55:32
8	you were simply defining the scope of the term	17:55:36
9	"cryptographic key information," that that term	17:55:40
10	includes certain things like keys -- defining the keys	17:55:44
11	or encryption type?	17:55:50
12	A. I mean, clearly the patent is saying that	17:55:53
13	cryptographic key information could include those	17:55:57
14	things, but I don't think that it's exclusive saying	17:56:00
15	that's all it could contain, this is just examples of	17:56:03
16	things that could be contained within that claim	17:56:05
17	term.	17:56:08
18	Q. All right. And so that's why you said "and." Right?	17:56:08
19	Because you're just enumerating some examples that are	17:56:11
20	within the scope of this term.	17:56:15
21	A. Correct.	17:56:16
22	MR. LU: Okay. No more questions.	17:56:18

1 MR. TEHRANCHI: All right. We're done.

17:56:22

2 (Proceedings concluded at 6:56 p.m.)

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

CERTIFICATE OF NOTARY

STATE OF MICHIGAN)

) SS

COUNTY OF OAKLAND)

I, ALISON WEBSTER, certify that the deposition of John Black, Jr. Was taken before me via videoconference on the date hereinbefore set forth; that the foregoing questions and answers were recorded by me stenographically and reduced to computer transcription; that this is a true, full, and correct transcript of my stenographic notes so taken; and that I am not related to, nor of counsel to, either party nor interested in the event of this cause.



ALISON C. WEBSTER, CSR-6266, RPR, RMR, CRR, RDR

Notary Public, Oakland County, Michigan

My commission expires: May 1, 2029

ACKNOWLEDGMENT OF DEPONENT

I, John Black, Jr., do hereby acknowledge
that I have read and examined the foregoing testimony
and the same is a true, correct, and complete
transcription of the testimony given by me and any
corrections appear on the attached errata sheet signed
by me.

(SIGNATURE)

(DATE)

A			
a-b	acceptable	86:14	algorithm
28:15	55:5	adding	11:11, 13:14,
a-s-i-a-n	access	26:17, 64:2	14:2, 14:4,
81:14, 81:20	9:10, 9:20,	addition	25:17, 33:15,
abiding	10:2, 10:8,	47:8	33:17, 33:21,
30:4	10:22, 11:3,	additional	36:6, 36:20,
ability	11:8, 12:6,	25:11, 26:12,	37:1, 53:21,
24:16, 24:19	12:12, 12:17,	26:18, 50:8,	54:6, 55:8,
able	14:2, 14:14,	75:9, 86:17	55:12, 56:9,
11:1, 12:5,	14:15, 15:3,	administered	59:12, 61:9,
13:1, 17:18,	72:20	5:7	63:5, 64:18,
18:13, 24:10,	accessed	admissibility	68:6, 90:19
24:11, 24:12,	10:6, 42:13	5:12	algorithms
27:4, 38:12,	accessing	advance	50:15, 56:1,
67:19, 68:3,	9:8, 10:13	86:13	56:6, 62:18,
69:13, 73:15,	according	aes	62:22, 64:18,
74:1, 74:20	18:22, 76:1,	13:17, 13:22,	64:21, 68:22
about	77:14, 91:16	14:2, 29:5,	alison
6:2, 9:7,	account	59:12	1:22, 2:8,
14:17, 15:18,	75:13	affects	96:6, 96:20
15:21, 16:8,	acknowledge	8:5	all
17:10, 22:10,	97:4	affirm	7:8, 8:12,
28:1, 30:20,	acknowledgment	5:8, 6:1	8:16, 13:18,
32:2, 36:14,	97:1	after	13:22, 18:9,
39:16, 42:5,	action	6:5, 63:4,	19:7, 24:6,
42:15, 44:18,	10:18, 44:1	64:10, 88:6	26:7, 26:20,
47:3, 47:4,	actors	again	26:21, 30:4,
47:13, 56:2,	44:6	9:5, 9:10,	34:2, 42:16,
57:2, 60:3,	actual	16:17, 28:4,	44:12, 45:5,
63:8, 65:6,	64:12, 74:18,	32:20, 49:13,	45:22, 46:2,
65:7, 67:1,	77:1	50:12, 54:3,	47:10, 50:17,
69:20, 70:5,	actually	75:1, 75:11,	51:10, 52:4,
70:12, 71:3,	14:21, 18:21,	78:7, 81:3	52:18, 57:16,
71:10, 72:10,	20:2, 20:4,	against	57:18, 58:8,
73:5, 80:1,	21:20, 36:11,	23:7	58:13, 60:6,
80:6, 83:16,	44:2, 57:11,	age	66:2, 67:4,
84:8, 85:18,	58:10, 62:14,	80:2, 80:12,	67:10, 67:15,
87:22, 88:22,	66:15, 68:9,	83:10, 83:11,	67:22, 68:5,
92:20, 93:1,	71:9, 77:6,	83:12, 85:7,	68:7, 71:4,
93:6	78:5, 84:11,	86:16, 87:2	73:6, 73:8,
above-styled	86:19, 87:15,	ago	74:20, 75:18,
2:6	88:17, 91:13,	78:15	81:8, 81:12,
absolute	92:5	agree	83:20, 94:15,
74:14, 75:2,	add	37:22, 53:18,	94:18, 95:1
78:1, 78:16	23:4, 28:22,	54:15, 60:10,	allocate
absolutely	64:21, 76:9	62:17, 69:1,	44:10
63:2	added	74:10	allow
	25:12, 76:17,	ahead	30:22
		50:22, 51:9	

allowed 23:4, 34:12, 34:13, 38:4, 74:18 allowing 37:11, 77:5 allows 67:14 alluded 16:21, 31:5 almost 10:10, 41:2, 41:3 alphanumerics 25:21 already 6:17, 73:4, 74:17, 75:10, 92:6 also 7:2, 9:3, 10:3, 11:20, 14:18, 19:11, 20:11, 22:15, 24:2, 29:20, 32:20, 36:14, 37:2, 44:4, 47:20, 49:9, 52:2, 52:15, 52:20, 58:5, 59:17, 60:13, 61:6, 61:19, 64:7, 65:7, 66:4, 80:20, 90:12 although 60:11 always 19:17, 25:19, 65:21, 66:2 amazon 11:16, 26:20, 47:15, 47:16, 90:20 ambiguity 9:21, 14:22 ambiguous 48:2 amenable 29:11	among 87:2, 91:19 amount 64:2 amounts 64:5 ampersand 88:5 analog 69:10 another 12:5, 13:1, 28:13, 31:14, 61:4, 63:12, 64:21, 76:9 answer 28:10, 36:1, 70:6, 70:15, 71:4, 82:1, 82:4, 82:22, 84:5, 86:8, 86:9, 90:15, 92:8 answered 92:6 answers 52:4, 79:6, 96:9 anticipate 7:16, 85:21, 85:22 any 5:11, 5:15, 7:5, 7:12, 15:13, 17:5, 22:3, 26:12, 26:16, 26:17, 27:6, 27:7, 28:1, 35:7, 39:2, 40:7, 44:8, 47:19, 48:14, 63:16, 69:13, 76:12, 94:3, 97:7 anymore 14:8, 38:13, 65:19, 94:1 anyone 58:7, 59:17	anything 7:2, 10:10, 25:2, 25:5, 31:19, 41:3, 42:15, 49:13, 58:10, 86:12 anywhere 27:7, 70:11, 71:5, 76:8 appeal 1:4 appear 81:9, 81:14, 82:6, 83:14, 86:8, 86:10, 97:8 appearance 5:14 appearing 3:3, 3:14 appendix 20:12, 71:10, 71:12, 71:20, 72:1, 79:19, 84:7 applied 65:9 applies 35:21 apply 38:17, 56:14, 57:17, 69:3, 75:21 approximation 70:17 april 1:16, 5:2 area 32:22, 43:11, 64:8 argumentative 43:1 arrange 25:22 arrangement 5:11 arrived 19:5	art 35:1, 40:13, 62:17, 84:22 asian 80:2, 80:13, 80:18, 81:18, 82:5, 82:14, 82:15, 82:17, 86:16, 86:22, 87:5, 87:6 asked 20:14, 78:17 asking 27:1, 77:20, 91:22 asks 58:11 aspects 17:10 assessment 62:20 assign 9:22, 15:20 assigned 14:19, 15:5, 15:9, 16:1, 16:4, 16:6, 16:20 assigning 15:1, 15:14, 15:16, 16:10, 16:16, 16:17, 17:6, 53:4 assigns 17:4 associated 41:17, 42:11, 42:12, 42:18 assume 33:16, 56:3 assuming 14:5, 26:10, 33:15, 50:3 asterisk 25:2, 25:3, 27:5 asterisks 30:15
--	--	---	---

asymmetric 58:21, 90:18 asymmetric-key 36:6 attached 2:13, 20:12, 51:4, 97:8 attack 34:12, 34:15 attacked 13:10 attest 78:16 attorneys 5:4 attributes 91:19 audio 69:5, 69:7, 69:10, 69:12, 70:3, 70:6, 70:22 augment 26:20 author 43:22, 52:9 automatically 25:10 available 40:17 avenue 3:17 avoids 30:2 aware 40:15 away 14:11, 30:18 awkward 29:15 B babak 3:4, 5:17 back 28:4, 39:11, 39:14, 42:8, 48:3, 54:3,	58:15, 66:21, 68:14, 73:9, 76:3, 79:17, 85:6, 90:21 backslashes 31:1 bad 31:4 bar 23:21, 25:3, 25:18, 25:22, 26:4, 27:5, 27:6, 27:7 bars 24:22, 25:6 base 25:20, 29:18 based 9:20, 16:20, 24:10, 31:3, 31:12, 32:22, 37:21, 48:9, 48:10, 49:6, 49:14, 49:18, 50:6, 50:10, 50:20, 55:17, 56:1, 63:5, 68:21, 92:4, 92:13, 93:5 basic 18:18 basically 9:11, 11:17, 12:13 basis 54:21 beauties 58:21 became 63:20 because 6:20, 9:6, 14:3, 24:6, 29:15, 30:15, 43:21, 45:5, 45:17, 46:1, 47:16, 51:1, 51:13, 51:21,	52:13, 52:19, 53:7, 54:8, 57:7, 62:13, 64:2, 65:1, 65:3, 65:15, 66:2, 67:19, 68:3, 68:7, 71:15, 76:3, 76:19, 77:1, 77:5, 77:20, 81:7, 86:10, 87:15, 94:19 become 46:15 been 6:6, 7:22, 14:3, 40:15, 71:14, 83:6, 93:14 beep 69:12, 69:14 before 1:4, 2:8, 7:13, 17:19, 26:3, 28:12, 28:19, 30:2, 63:9, 75:11, 87:8, 90:14, 96:7 beginning 48:3, 48:19, 72:1 begins 23:15, 24:6, 28:13 behalf 3:3, 3:14, 58:12 being 13:2, 13:19, 17:18, 23:20, 26:22, 29:11, 33:17, 33:21, 35:3, 35:6, 90:19, 90:22 believe 13:16, 37:2, 40:15, 41:19, 82:21, 85:2	belonging 16:6 below 53:7 benefit 36:7, 66:4 benefits 35:1 benign 61:20 better 13:16 between 23:18, 25:6, 44:9, 59:14, 67:16, 82:16, 87:12 beyond 16:12, 17:2, 18:18, 22:21, 70:18 big 66:17 binary 12:22, 29:8, 29:14 bit 17:9, 17:22, 32:1, 34:4, 34:5, 39:16, 60:7, 62:13, 63:8, 66:22, 68:9, 71:17, 79:7, 80:15 bits 25:19, 29:6, 29:7, 64:3, 66:12, 68:2 black 1:15, 2:4, 4:4, 5:1, 5:6, 5:21, 6:4, 6:15, 34:11, 39:16, 42:15, 79:19, 89:16, 96:7, 97:4 board 1:4
--	--	--	---

boolean 80:1, 81:9, 88:5 both 13:21, 35:20, 47:2, 57:20, 59:16, 64:14, 81:9, 86:8 bother 79:5 bottom 72:2 boundaries 9:15 box 14:7, 14:14, 34:11 brain 67:19 break 7:6, 8:7, 21:6, 39:7, 39:9, 62:18, 63:4, 79:10 breaking 61:20, 63:1, 68:13, 68:14 breaks 8:7 broad 41:2 broader 17:10, 19:22 broken 13:9, 13:17 brute-force 33:14, 34:1, 34:8, 34:10, 34:17 btehranchi@perki- nscoie 3:11 bucket 43:11 buckets 11:16 build 15:19, 24:17	built-in 24:16, 24:19 bunch 11:6, 11:7, 25:1, 87:5, 87:7 burden 59:5 C c 63:13 california 3:9 california) 2:9 called 6:5, 33:18 camino 3:7 can't 23:22, 29:16, 29:22, 58:10, 58:14, 60:4, 64:6, 65:2, 68:4, 68:6, 77:4, 78:15, 86:4 cannot 28:21, 77:17 capable 59:17, 59:18 car 86:1, 86:3, 86:7, 86:10 cards 26:8 care 28:1 carrying 91:19 case 1:12, 13:5, 29:13, 35:22, 38:11, 57:13, 59:12, 59:15, 59:18, 73:11, 73:14, 76:22, 78:11, 82:21,	93:18 cases 36:5, 64:14 categorization 81:21 cause 2:6, 96:15 caveat 78:13, 81:3 certain 11:3, 18:22, 22:15, 28:20, 28:21, 31:1, 40:17, 64:3, 76:13, 94:10 certainly 15:7, 16:11, 16:14, 17:3, 17:14, 31:16, 35:21, 39:1, 59:4, 61:15, 62:22, 66:17 certainty 78:16 certificate 90:21, 96:1 certify 96:6 change 13:6, 13:12, 13:20, 14:10, 31:3 changed 13:6, 14:6 character 23:19, 26:2, 26:4, 26:5, 27:20, 66:13 characterize 74:19 characters 22:16, 24:4, 25:9, 25:13, 27:16, 27:21, 28:21, 29:2, 30:14, 66:12, 66:15, 66:18 cheat 18:12	check 21:19 choice 31:4 choose 27:14, 27:18 chosen 34:12 chunk 48:8, 48:16, 49:6, 54:21, 55:17, 56:4, 57:14, 59:16, 59:17, 59:18, 59:19, 59:21, 62:19, 63:11, 63:12, 63:22, 64:13 chunks 14:16, 19:14, 19:19, 21:6, 21:9, 21:13, 44:2, 44:20, 44:21, 45:3, 49:12, 49:15, 50:19, 52:16, 52:17, 53:10, 53:12, 53:14, 55:8, 56:1, 56:14, 56:22, 57:17, 57:18, 58:8, 58:14, 59:2, 59:13, 60:10, 61:12, 61:21, 62:1, 62:5, 62:10, 62:12, 62:19, 63:1, 63:4, 63:10, 65:7, 66:13 ciphertext 7:19, 7:21, 25:17, 29:10, 32:7, 32:10, 32:16, 32:19, 33:1, 33:6, 33:9, 33:14, 34:1, 34:10,
--	--	---	---

34:14, 34:17, 59:21, 63:18, 64:1, 64:9, 64:14, 65:16, 65:18, 76:1, 76:18, 78:9, 78:10, 79:1, 87:6, 87:7 circumstances 57:5 civil 2:12 claim 9:3, 14:18, 15:1, 15:16, 16:3, 16:9, 16:14, 17:3, 19:21, 31:17, 36:22, 37:10, 37:15, 38:3, 38:4, 38:9, 52:20, 53:1, 53:3, 54:3, 55:9, 55:13, 56:2, 56:4, 60:11, 60:18, 62:3, 62:7, 62:9, 62:14, 68:15, 84:11, 85:13, 88:16, 88:17, 90:10, 91:10, 91:22, 93:20, 94:16 claimed 69:4 claims 14:20, 23:2, 31:12, 31:13, 31:16, 36:19, 37:7, 37:8, 68:21, 70:20, 84:9, 84:10 clarify 6:18 class 15:10, 16:21 classifies 82:15	clear 7:4, 9:14, 9:19, 18:1, 46:9, 48:1, 52:11, 68:19, 93:5 clearer 93:14 clearly 38:3, 87:12, 94:12 cloud 10:3, 11:16, 11:18, 15:4, 21:8, 21:9, 24:19, 26:11, 26:12, 26:17, 27:9, 27:17, 27:18, 29:21, 30:3, 30:8, 31:3, 35:4, 38:13, 38:17, 38:20, 38:22, 39:2, 41:17, 42:4, 42:11, 43:3, 43:5, 43:10, 43:16, 44:4, 44:10, 47:5, 47:7, 47:9, 51:19, 57:22, 59:14, 59:21, 60:5, 61:11, 72:19, 73:11, 73:14, 73:22, 74:17, 74:20, 75:15, 75:19, 76:22, 77:3, 77:7, 78:6, 79:1, 79:4, 83:18, 85:9 cloud's 24:16, 58:13 clue 13:4 code 20:10, 20:14, 20:19	coie 3:6 column 41:13, 42:8, 72:11, 81:15, 91:16, 92:7 columns 81:17 com 3:11, 3:12, 3:21 come 39:11, 63:18 comes 63:9, 78:2 comma 23:21 commission 96:22 common 40:14, 63:17 company 13:15, 13:18, 81:11 complete 47:18, 97:6 compound 84:3 comprise 66:18 comprised 16:2, 81:7 comprises 37:11 compromised 14:12 computer 12:15, 13:1, 23:17, 34:6, 40:14, 47:22, 96:11 computers 44:9 concatenated 21:21 concept 17:18, 33:5, 40:14	conceptually 47:1 concerned 27:20 concluded 95:2 concludes 34:21 conditions 11:3, 81:9 conducting 87:15 conferences 18:11 configuration 12:14, 12:16, 13:3 configure 10:3, 23:2, 85:14 configured 11:21, 23:5, 60:20 configuring 9:8, 48:5, 49:3, 53:13 confirm 82:22 confuse 30:16 confusion 19:8 connect 90:20 connection 49:16, 51:5 consent 5:10 consider 32:22 considerations 30:6 considered 16:7, 33:2 constituent 93:17 constitute 66:19
---	--	---	---

constraint 22:12, 67:13 contain 94:15 contained 22:8, 91:22, 94:16 container 27:8, 40:3, 41:9, 42:6, 43:4, 43:6, 43:12, 46:6, 46:7, 52:6 containers 41:15, 41:21, 42:10, 42:17, 44:3, 52:14 containing 90:3 contains 58:12 content 9:8, 10:2, 10:6, 10:7, 18:7, 42:12, 42:19, 53:6, 54:4, 54:5, 85:14 contents 13:4, 18:19, 27:22, 54:16, 54:20, 77:1 context 12:13, 40:17, 41:20, 45:18, 45:21, 46:4, 46:10, 46:22, 47:2, 47:4, 47:14, 47:22, 48:1, 67:3 continue 39:9, 79:19 control 12:6, 12:7 convention 49:12 conversation 7:4	conveys 93:8 copy 7:9 correct 7:15, 8:10, 9:1, 9:2, 9:12, 10:7, 15:6, 17:16, 18:2, 18:7, 18:19, 21:16, 24:12, 28:7, 28:19, 29:3, 31:10, 31:14, 32:8, 32:9, 32:16, 32:18, 35:19, 36:20, 38:20, 48:20, 54:21, 56:3, 60:9, 60:13, 61:12, 62:13, 63:6, 63:13, 73:16, 73:21, 83:15, 93:10, 94:21, 96:12, 97:6 corrections 7:12, 7:17, 97:8 correctly 73:12, 74:2, 75:16, 77:8, 77:10 corresponded 7:19 corresponding 56:15, 57:1, 57:7 corresponds 57:17 could 7:4, 8:19, 10:10, 11:11, 11:15, 11:20, 16:20, 19:6, 20:15, 20:22, 21:15, 21:20, 22:16, 24:2, 27:1, 28:21,	31:8, 31:9, 34:9, 37:2, 37:3, 38:21, 40:3, 40:19, 42:6, 47:16, 47:20, 50:5, 56:14, 57:3, 57:4, 57:16, 58:4, 58:5, 58:15, 58:16, 58:18, 58:20, 61:9, 63:10, 63:12, 63:18, 64:14, 64:20, 64:21, 65:1, 65:9, 66:5, 67:14, 67:18, 68:9, 69:7, 69:8, 69:14, 70:21, 71:19, 82:5, 82:6, 82:8, 84:19, 85:11, 86:6, 86:8, 86:22, 87:1, 87:13, 90:3, 92:20, 92:21, 92:22, 94:13, 94:15, 94:16 couldn't 22:12, 70:14, 86:9 counsel 5:10, 5:14, 5:16, 5:17, 5:19, 92:10, 94:3, 96:13 counted 9:17 county 96:4, 96:21 couple 7:18 course 20:10, 27:15, 52:21, 66:1 covering 69:22	covers 16:17, 35:20 create 21:8, 22:7, 41:9, 42:21, 43:3, 43:10, 43:12, 45:5, 45:7, 45:9, 45:11, 46:12, 46:22, 47:7, 49:11, 51:17, 51:21, 52:3, 52:6, 53:21, 54:7, 67:2 created 41:6, 41:21, 42:2, 42:16, 46:1, 50:4, 50:6, 50:11, 50:12, 51:14, 52:10, 64:8, 71:16 creates 43:4, 43:15, 44:20, 45:2, 75:7 creating 43:8, 43:20, 44:5, 45:4, 48:5, 49:2, 49:15, 51:3, 51:12, 53:11, 53:16, 67:1 creation 42:3, 42:6, 44:12, 48:16, 50:18, 51:4, 52:13, 52:18 crr 1:22, 2:8, 96:20 cryptographic 37:17, 88:20, 89:1, 89:5, 89:10, 89:17, 89:20, 90:9, 91:3, 91:6, 91:10, 92:2,
--	---	--	--

92:15, 92:18, 93:9, 93:18, 94:9, 94:13 cryptography 33:16, 35:16, 36:2, 36:6, 58:22, 59:6 csr 1:22, 2:8, 96:20 cybertexts 65:2	19:3, 40:22, 44:14, 48:21, 71:7, 84:14, 85:18, 88:10, 89:19, 91:12 decrypt 18:12, 57:18, 58:19, 59:16, 60:5, 73:12, 74:1, 74:2, 74:21, 75:16, 77:8 decrypted 77:10 decrypting 18:6, 18:15, 58:17, 59:18, 87:8 decryption 57:1, 57:8, 58:1, 58:20, 59:5, 77:2, 77:13, 89:6, 89:12, 89:22, 91:18, 93:19 decryptions 75:18 deep 33:12 define 10:5, 11:20, 40:7, 45:8, 90:4, 91:4, 91:17, 93:8 defined 48:9, 49:7, 88:20, 89:1, 91:6, 91:7, 91:11, 93:19 defines 8:22, 9:20, 10:1, 10:17, 49:11, 54:12, 54:13 defining 89:6, 89:21, 90:2, 94:8, 94:10	definition 39:20, 40:10, 90:8 delimited 28:18 delimiter 27:20 delimiters 26:14, 26:15, 27:10, 27:14, 27:16, 28:6, 28:9 delineated 23:10 demanding 30:13 depend 34:3 dependent 31:17, 37:7, 38:4 depending 69:7 depends 34:16, 37:15, 51:14, 64:18, 83:4 depiction 59:22 depicts 42:3 deponent 97:1 deposit 59:20 deposition 1:15, 2:4, 5:1, 5:5, 7:13, 71:10, 96:7 describe 20:6, 39:17, 47:14, 76:10 described 10:16, 20:16, 68:22, 69:4, 84:3 describes 37:3, 51:3,	92:20 describing 19:20, 36:8, 48:16 description 47:18, 67:14, 68:22 design 59:9 designation 81:22 desired 59:22 desires 13:15 details 20:7, 20:12, 20:22, 81:4, 85:19 deterministic 65:21 device 12:4, 12:5, 15:2, 16:22, 17:4, 26:11, 26:13, 26:17, 35:5, 35:7, 37:12, 38:1, 38:2, 38:6, 38:8, 59:7, 60:1, 88:20 diego 3:9 different 7:22, 9:17, 11:6, 11:7, 13:11, 18:9, 27:18, 30:7, 30:8, 31:7, 34:15, 36:3, 45:4, 54:14, 55:2, 58:18, 62:7, 64:15, 65:1, 65:3, 65:11, 72:10, 81:13, 82:5, 83:6 difficulty 62:13
--	--	--	--

digest 12:8, 13:2 digit 45:20 directed 84:1 directly 54:17 directories 40:6, 41:16, 42:10, 42:18 directory 40:8, 46:8, 46:12, 46:15 disagree 74:10, 77:21 disagreed 62:6 disavowal 71:5 discard 80:11 disclosed 18:17 disclosure 74:15, 75:3, 78:2 disk 44:11 distinct 12:2 distribute 21:7 divide 62:4 dividing 53:10, 62:10 document 12:9, 21:4, 29:12, 79:8, 80:18, 81:1, 82:6, 83:14, 89:14, 91:9, 92:17, 93:13 documents 12:16, 13:19, 14:1 doing 19:20, 20:4,	28:1, 43:13, 62:14, 81:6, 88:4, 88:8, 90:18 domain 64:9 done 26:22, 31:18, 54:21, 58:20, 70:14, 82:5, 95:1 down 7:17, 66:9, 67:17, 81:16, 83:7 download 37:3, 37:11, 38:5, 38:7, 57:16 downloaded 37:16, 38:1, 38:22 dr 5:21, 6:15, 39:16, 42:15, 79:19, 89:16 dragonfruit 20:17, 71:15, 83:3, 86:18, 88:1 drives 44:11 duly 2:5, 6:6 duplicative 9:7 during 8:6, 71:9	86:6, 88:4 earlier 6:20, 16:21, 31:5 eastern 2:7 easy 33:8, 75:15 efficient 87:4 either 23:18, 29:11, 35:22, 76:18, 84:19, 85:11, 96:14 el 3:7 elaborate 80:16 email 29:12 emails 29:17 emanuel 3:16 embedded 34:11 embodied 11:4 embodiment 19:21, 23:1, 24:15, 26:19, 36:16, 91:12, 91:17, 92:7, 92:9, 93:15 embodiments 15:13, 21:20, 43:9, 51:10, 60:14, 60:16, 85:19 encode 25:20, 25:21, 26:2, 29:10, 30:1, 30:14, 81:12 encoded 12:21, 81:10 encoding 11:4, 12:22,	29:17, 29:18, 29:19, 30:12, 72:5 encompasses 41:2 encrypt 21:12, 29:5, 35:11, 49:6, 54:16, 55:8, 55:22, 56:14, 56:21, 58:8, 58:18, 59:16, 59:19, 60:19, 63:5, 63:22, 64:5, 64:13, 64:22, 74:16, 84:16, 84:17, 85:10, 85:11 encrypted 9:9, 11:11, 11:14, 13:19, 17:18, 18:2, 18:5, 18:6, 18:14, 18:19, 21:7, 21:10, 24:3, 26:1, 26:10, 28:12, 31:6, 32:6, 35:1, 35:8, 35:15, 36:13, 36:17, 37:12, 37:16, 38:5, 38:9, 42:13, 44:19, 48:8, 50:20, 55:17, 57:14, 58:13, 59:20, 60:11, 60:13, 60:15, 60:17, 60:20, 61:7, 62:12, 63:11, 64:11, 65:11, 68:15, 68:21, 72:20, 74:17, 75:10, 75:11, 79:3, 83:19, 83:21, 84:15, 85:15, 86:1, 87:14,
---	--	--	--

88:3 encrypting 28:22, 53:8, 54:3, 54:5, 54:10, 54:20, 57:6, 59:17, 62:3, 62:8, 65:7, 65:8, 65:10, 79:5, 88:19 encryption 10:15, 11:12, 13:9, 13:11, 14:2, 17:13, 17:15, 18:1, 18:21, 25:17, 26:22, 31:7, 33:1, 33:3, 33:5, 35:21, 36:21, 48:6, 48:10, 48:15, 49:3, 49:7, 49:14, 50:15, 51:19, 52:15, 52:17, 52:19, 53:5, 53:16, 54:6, 55:7, 56:4, 56:21, 58:19, 59:13, 60:8, 61:3, 61:16, 62:1, 62:18, 62:22, 63:9, 63:16, 65:20, 65:21, 70:1, 70:7, 72:12, 72:17, 72:18, 78:9, 84:11, 85:17, 87:17, 89:6, 89:7, 89:12, 89:22, 90:12, 90:16, 90:17, 90:22, 91:5, 91:18, 91:20, 93:1, 93:7, 93:9, 93:19, 93:20, 94:11 encryption-key 53:21	end 26:15, 36:10, 39:6, 60:1, 67:7, 71:22 endpoint 59:7 ends 23:15, 24:6, 25:11 engineer 33:8, 33:12 engineering 31:4, 59:10, 61:2 enjoying 39:2 enough 20:1, 20:13, 30:13, 34:18, 38:14, 45:7, 45:11, 45:14, 45:15, 66:20, 70:4, 71:6, 79:6, 82:3, 83:9, 88:9, 88:13, 93:4, 93:22 entire 76:6, 76:9, 76:16, 81:4, 86:20 entity 43:15 enumerate 68:6 enumerating 94:19 envelope 30:21 equals 86:22, 87:5 errata 97:8 errors 7:18 esquire 3:4, 3:5, 3:15 essence 52:10	est 1:17 established 45:17 even 11:13, 12:5, 12:21, 24:3, 34:6, 38:22, 47:12, 47:15, 51:18, 52:1, 52:5, 64:10, 64:22, 68:6, 76:12, 81:7, 84:5 event 96:14 ever 68:10, 69:21 every 22:10, 24:5, 64:19, 93:18 everything 13:21 everything's 7:4 exact 14:21, 83:3 exactly 9:14, 71:8 examination 4:6, 4:8, 6:13, 94:5 examined 6:8, 97:5 example 10:21, 13:7, 14:7, 17:1, 23:11, 25:19, 32:4, 32:10, 33:22, 36:7, 36:11, 36:12, 39:19, 39:21, 39:22, 40:2, 40:19, 41:10, 41:12, 41:16, 42:6, 43:19, 47:5, 48:5, 48:7, 49:2, 49:5, 55:16, 57:19, 60:22, 61:8, 63:11, 63:19, 69:11, 80:7, 80:19, 82:7, 85:6, 86:18, 87:11 examples 15:13, 41:7, 94:15, 94:19 exceed 22:13 exclusive 40:19, 94:14 execute 11:2 exhibit 4:13, 6:19, 6:22, 7:10, 37:8, 71:12, 79:20 exhibits 4:15, 6:16 exists 57:10 expand 66:16 expands 64:1 experience 83:15 expert 70:10 expires 96:22 explain 41:5, 46:10, 50:5, 55:7, 73:10 explained 74:11 explains 8:18 explanation 48:14, 50:3, 78:5 explicit 23:6
---	--	---

explicitly 10:8, 39:19, 41:7, 52:8 extent 71:13, 84:20 F facilitate 60:20 facilitating 61:6 facility 57:22, 59:14, 83:18, 85:9 fact 32:18, 53:19, 63:20, 64:8, 65:14 fair 20:1, 20:10, 34:18, 38:14, 42:22, 43:2, 50:9, 62:19, 66:20, 70:4, 70:19, 71:6, 73:1, 79:6, 82:3, 83:9, 83:12, 88:9, 93:4, 93:22 fairly 8:15, 19:6, 61:20 fall 61:6 familiar 70:16, 71:11, 71:13, 73:4 far 27:20, 54:20 fast 34:6 faulty 13:14 feature 75:6, 76:9, 76:17 federal 2:12	feel 8:15, 44:17, 72:8 few 8:4, 44:6 fields 22:19 figure 41:15, 41:20, 41:22, 42:1, 42:3, 42:9, 42:17, 62:15, 70:2 filename 44:19, 54:11, 54:17, 55:1, 55:4 filenames 19:14, 19:19, 20:3, 20:8, 45:19, 46:14, 52:20, 52:21, 54:12, 54:14, 86:2 files 11:2, 14:3, 14:11, 37:4, 37:22, 40:7, 41:16, 42:10, 42:13, 42:18, 45:12, 45:14, 45:22, 46:2, 46:3, 46:17, 47:6, 47:9, 49:15, 61:20, 69:7, 69:21, 70:6, 70:21, 70:22, 71:5 filing 17:19 filipino 80:20, 82:8, 82:12, 82:17 final 72:16, 72:18 find 8:7, 11:13, 25:14, 47:20, 87:10, 92:21 finds 58:12 first 3:17, 6:6, 9:3, 28:15, 49:1, 50:10, 50:17, 53:3, 53:9, 62:4, 62:9, 62:18, 65:17, 70:17, 78:8, 79:5, 86:16, 90:14 fit 64:10 five 9:6, 9:11, 9:17, 39:7 fix 8:3 fixed 24:3, 31:8, 31:20, 64:2 focus 8:16 folder 27:8, 40:8, 44:19, 44:20 folders 40:7, 41:16, 42:10, 42:18 follow 75:15 follow-up 8:20 follows 6:8 followup 92:9 forbidden 22:15, 23:19, 25:9, 25:13, 26:1, 28:21, 29:2 force 61:1 foregoing 96:9, 97:5	forestall 61:2 forget 75:10 forgot 71:7 form 19:13, 85:1, 89:18 format 12:21, 69:7 forth 96:9 fortinet 1:9, 5:20 forward 58:15 found 25:7, 57:15 four 32:20, 72:10, 72:15, 73:6 four-letter 32:13 fourth 72:12 free 8:16, 44:17, 72:8 friday 2:6 front 7:11 frown 33:19 full 50:12, 79:22, 96:11 function 66:1, 66:4 functions 66:9 further 7:3, 20:11, 48:14, 79:7 future 85:22 G gateway 9:22, 12:4,
--	---	--

15:2, 17:4, 32:6, 35:5, 43:17, 44:9, 56:20, 56:22, 57:3, 58:7, 58:9, 58:11, 58:14, 58:20, 59:8, 59:14, 59:19, 60:1, 72:21, 74:15, 77:13, 88:19 gave 20:15, 68:11 gears 17:9 general 11:8, 18:13, 84:13 generalize 84:8 generally 32:16 generate 30:7, 32:6, 54:7 generated 65:17 generating 56:10 generic 30:17 gentle 30:13 getting 87:16 give 6:2, 11:8, 12:17, 13:7, 23:11, 47:18, 48:1, 68:2, 76:17, 79:3, 85:19 given 57:4, 59:21, 68:8, 70:13, 97:7 gives 20:11, 20:13	giving 60:3, 90:5 glass 39:11 global 45:22 go 8:12, 14:20, 14:21, 19:2, 20:22, 34:19, 37:8, 39:8, 39:10, 42:8, 43:10, 44:2, 44:14, 48:7, 48:15, 49:5, 50:9, 50:22, 51:9, 51:17, 52:14, 54:14, 54:18, 55:15, 66:2, 70:2, 71:17, 71:20, 71:22, 84:4, 85:6, 88:16 gobbledygook 29:8 goes 18:18, 26:10, 32:3, 88:2 going 8:2, 11:19, 14:1, 22:7, 24:15, 26:19, 27:14, 28:4, 29:6, 29:7, 29:8, 30:12, 32:2, 32:20, 34:8, 35:14, 41:22, 43:9, 46:13, 50:14, 50:15, 54:3, 66:18, 66:19, 71:19, 81:16, 86:18 gonna 6:15 good 7:7, 18:10, 39:6, 65:4, 66:2	gosh 13:18 grabs 81:11 great 7:12 greater 80:2, 83:11, 83:13, 86:17, 87:2, 87:6 group 15:9, 15:14, 15:15, 15:19, 16:1, 16:4, 16:5, 16:7, 16:10, 16:15, 16:16, 16:18, 46:2 groups 15:19, 15:20, 15:22 grow 64:10 grows 63:19, 64:4 guess 15:7, 81:19, 81:22, 87:10 H hand 5:22, 54:18 handle 25:4, 84:2 hands 51:17 happen 78:19 happens 13:5, 22:2 happy 39:10 hard 34:2, 34:17 hardware 35:4, 38:13, 38:16 hash 60:22, 61:1,	61:9, 66:1, 66:4, 66:7, 66:9 hashes 66:6 hazard 81:19 head-scratching 12:22 heading 72:7 headings 72:15 heard 17:12 heavier 59:5 hence 44:18 here 10:21, 13:19, 42:16, 42:20, 44:7, 45:2, 48:16, 50:11, 50:19, 51:19, 60:9, 61:19, 69:22, 70:14, 78:8, 84:3, 84:5, 85:4, 88:12, 88:22, 92:4, 93:5 here's 27:2, 41:8, 43:2, 43:3 hereby 97:4 herein 6:5 hereinafter 19:12 hereinbefore 96:8 hereto 2:13 hey 27:1, 51:16 hidden 33:18 hide 61:15, 77:4
---	---	--	--

highly 65:14 hinting 28:12 hit 76:19 hits 77:3 hold 21:9, 42:4, 84:20, 90:6 hope 7:3 hosts 35:7 hour 79:10 however 12:9 human 12:20, 13:2, 43:22 hypothetical 10:20, 15:12, 30:10, 33:11, 55:11, 61:14, 63:15, 64:17, 81:2, 82:11, 87:20 I idea 11:8, 24:14, 68:12 ideally 12:1 identify 47:20, 67:4, 67:10 illinois) 2:10 image 70:22 imagining 25:15, 27:15, 28:8 implement 20:15, 26:16,	31:11, 85:20 implementation 22:10, 23:18, 27:15, 43:6, 47:13, 81:5, 91:15 implementations 82:8 implemented 18:22, 83:4, 83:6 implementing 20:2, 20:16, 25:16, 30:11, 88:5 implicated 44:4 important 74:14, 75:8, 78:1, 78:18, 78:20 inc 1:6, 1:9 include 15:14, 28:9, 56:5, 70:22, 89:11, 89:16, 90:12, 94:13 included 15:8, 21:21, 23:20, 46:18, 92:14 includes 89:5, 89:21, 94:10 incomplete 10:19, 15:11, 30:9, 33:10, 55:10, 61:13, 63:14, 64:16, 81:1, 82:10, 87:19 incorporation 84:21 indented 53:7 independent 31:16	index 35:7, 65:18, 80:14 indexes 31:6 indicate 47:14, 50:14, 67:12 indicated 21:11, 28:11, 46:16 indicating 12:2 indication 82:14 indices 19:11, 35:2, 72:5 individual 24:10, 54:21, 55:8 individually 83:19, 86:6, 88:4 inferring 75:4 infiltrated 14:7 influence 52:17 influenced 51:13 influences 43:21, 52:12 influencing 52:10, 54:17 information 12:3, 12:14, 20:13, 22:20, 37:18, 42:5, 47:20, 51:15, 52:7, 88:20, 89:1, 89:5, 89:10, 89:17, 89:21, 90:9, 90:21, 91:1, 91:4, 91:6, 91:7, 91:11,	92:1, 92:3, 92:15, 92:19, 93:1, 93:10, 93:16, 93:18, 94:9, 94:13 innocent 58:9 inoperable 65:15 input 66:3, 68:10, 68:12 insist 24:2 instance 2:5, 87:22 instances 69:13 instead 35:5 insulated 46:2 intended 13:1 interested 64:20, 76:13, 96:14 interesting 70:12, 71:2 interpretation 73:21, 82:7 interrupt 50:21 introducing 31:6 invention 31:13 involves 62:9 ipr 1:12 irrelevant 76:3 issues 7:14 item 36:7, 38:15, 90:17
--	---	---	---

Conducted on April 3, 2024

110

items 9:6, 9:12, 10:16, 38:15, 41:1, 89:17 itself 11:13, 13:14, 21:5, 23:20, 44:8, 63:20, 84:7, 92:21, 93:2 iv 72:4	58:1, 58:6, 58:8, 58:16, 59:15, 59:20, 61:2, 61:4, 72:21, 73:15, 74:1, 74:16, 75:12, 75:20, 76:18, 88:20, 89:1, 89:5, 89:10, 89:17, 89:21, 90:4, 90:6, 90:9, 91:1, 91:3, 91:6, 91:10, 92:1, 92:2, 92:15, 92:18, 92:20, 92:21, 92:22, 93:2, 93:9, 93:16, 93:18, 94:9, 94:13 keys 34:2, 36:15, 48:9, 48:10, 49:6, 49:7, 50:16, 52:16, 55:18, 57:3, 60:3, 79:4, 89:6, 89:12, 89:22, 91:18, 93:19, 94:10 keyword 28:13, 57:15, 58:12, 60:14, 61:1, 76:8, 86:4, 86:11, 86:12 keywords 19:12, 21:10, 22:13, 22:20, 26:1, 31:7, 35:8, 35:11, 36:13, 36:16, 60:12, 60:17, 60:19, 69:10, 69:15, 84:14, 84:18, 85:17, 85:21, 86:2	kind 18:11, 22:8, 36:22, 39:5, 57:12, 67:13, 70:7, 72:8, 73:4, 82:14, 84:8 kinds 8:3, 18:9, 69:17, 81:13 know 7:3, 7:6, 8:6, 8:8, 8:15, 10:9, 10:16, 11:5, 12:7, 12:8, 12:11, 12:18, 13:10, 13:18, 14:8, 15:13, 16:22, 19:3, 20:13, 20:21, 22:16, 23:4, 23:9, 23:14, 24:5, 25:2, 25:20, 26:6, 26:7, 26:13, 26:15, 26:20, 27:4, 27:19, 28:8, 28:12, 29:11, 29:14, 33:15, 33:17, 33:20, 33:21, 39:5, 39:8, 44:2, 44:7, 45:19, 46:5, 47:1, 48:21, 50:2, 50:13, 52:3, 52:5, 52:9, 57:10, 57:13, 59:4, 59:6, 61:8, 63:21, 66:10, 67:16, 67:17, 68:3, 68:10, 69:9, 69:16, 70:13, 70:17, 70:20, 77:18, 77:22, 78:13, 81:12, 81:13,	81:21, 83:3, 83:15, 84:4, 84:6, 85:22, 87:22, 88:7, 90:20, 92:6, 93:6, 93:15 knowledge 32:22 known 17:19, 71:1 knows 25:4, 25:8, 68:7
J		L	
job 1:19, 20:10 john 1:15, 2:4, 4:4, 5:1, 5:6, 6:4, 96:7, 97:4 jr 1:15, 2:4, 4:4, 5:1, 5:6, 6:4, 96:7, 97:4		language 14:20, 91:10 large 59:4, 66:9 larger 63:18 last 8:17, 8:21, 19:10, 44:18, 53:13, 72:16, 73:2, 74:13, 76:10, 77:14, 77:16, 78:18, 89:3, 92:13, 93:7 later 27:3, 57:15, 60:7, 76:1, 86:14 law 84:21 learn 77:1, 77:3 least 9:19, 12:1, 20:15, 36:22, 38:3, 43:9, 47:12, 48:20, 52:4, 52:13, 73:10, 75:8, 83:15, 89:5, 89:11, 89:21, 90:8, 93:16	
K			
keep 64:8 kept 28:18 key 11:12, 11:13, 33:14, 33:22, 34:1, 34:3, 34:4, 34:5, 34:11, 35:9, 35:12, 36:1, 36:11, 36:13, 36:17, 36:18, 37:17, 54:6, 56:1, 56:3, 56:6, 56:15, 56:16, 57:1, 57:4, 57:6, 57:7, 57:8, 57:14, 57:15, 57:17, 57:18, 57:20, 57:21,			

left 43:5, 72:10 length 11:12, 22:11, 24:3, 24:7, 31:8, 31:9, 31:19, 31:20, 32:17, 63:10, 63:13, 63:17, 92:22 lengths 33:6 let's 8:12, 13:7, 13:9, 13:17, 13:21, 15:22, 17:9, 17:22, 19:2, 20:20, 23:12, 23:21, 24:14, 24:21, 33:20, 34:19, 39:16, 53:18, 59:12, 61:3, 66:11, 66:21, 73:19, 74:10, 79:7, 79:11, 79:19, 79:20, 80:11, 80:12, 80:17, 83:10, 84:6, 84:8, 84:12, 85:6, 86:2, 88:9 letters 25:6, 30:18, 32:20, 32:21, 33:2, 63:20 leverage 24:15, 38:12 leveraged 38:16 license 2:9, 2:10 lieu 5:6 lifetime 34:6 limit 22:11, 22:14,	22:16, 68:15 limitation 16:3, 53:3, 53:8, 62:3 limitations 19:1 limited 35:7, 70:21, 82:20 limiters 26:5 limits 22:3, 22:8 line 41:13, 42:8 list 11:15, 14:13, 51:18 listed 9:12, 10:4, 36:8 lists 40:5 literal 81:20 literally 12:17, 82:12, 83:7 little 17:9, 17:22, 32:1, 39:16, 60:6, 62:13, 63:8, 66:21, 66:22, 71:17, 79:7, 79:10, 80:15 live 45:21, 46:5, 46:17, 46:18, 47:2, 47:21 lives 47:19 llp 3:6, 3:16 local 37:12, 38:1, 38:5, 38:7, 38:17	locally 37:4, 38:18, 39:1, 39:2 location 14:9, 47:8 logic 25:11, 26:12, 26:18 long 8:15, 17:6, 24:4, 33:2, 34:8, 34:21, 71:19, 88:14 longer 14:14, 32:1, 64:1 longwinded 82:1 look 12:8, 12:11, 24:16, 24:19, 25:2, 26:8, 26:13, 26:14, 27:3, 27:4, 28:15, 46:21, 52:2, 69:17, 80:12, 81:17, 87:2 looking 10:12, 13:2, 20:21, 24:21, 41:22, 81:19, 83:22, 94:7 lost 85:4 lot 29:15, 30:14, 62:17, 66:14 love 71:3 lowercase 30:18 lu 3:15, 4:9, 5:19, 9:13, 10:19, 15:11, 16:12, 17:2, 17:17, 18:8,	20:9, 21:4, 21:17, 22:6, 22:21, 23:16, 24:13, 27:12, 29:4, 30:9, 31:15, 33:4, 33:10, 35:13, 40:21, 43:1, 43:18, 49:19, 51:7, 54:1, 54:9, 55:3, 55:10, 56:12, 58:2, 59:3, 61:13, 62:2, 62:21, 63:14, 64:16, 65:13, 67:6, 68:17, 74:5, 74:22, 80:22, 82:10, 83:2, 84:20, 87:19, 89:13, 89:18, 91:8, 92:10, 92:16, 93:12, 94:4, 94:6, 94:22 M machine 46:20 made 32:19, 49:16 make 7:2, 7:13, 7:16, 14:21, 17:5, 21:2, 25:16, 28:18, 29:1, 29:19, 30:3, 52:14, 53:14, 59:10, 76:14, 87:9 makes 69:20, 70:2 making 23:13 man 80:20, 82:8, 82:13, 82:17 managed 48:10, 49:8
---	--	---	---

management 15:14, 15:19 managing 15:3, 37:10 manner 5:12, 5:15, 10:1, 10:5, 10:6, 11:21 many 22:12, 77:3, 83:6, 89:17 march 2:7 match 24:12, 65:19, 73:12, 74:2, 75:17, 76:20, 77:8, 81:17, 82:16, 87:7 matched 75:21 matter 5:8, 6:2, 8:2, 11:10, 84:18 matters 8:5 maybe 9:6, 9:16, 10:9, 11:13, 25:1, 30:18, 47:12, 57:3, 59:7, 60:22, 62:6, 64:4, 66:21, 69:8, 69:14, 70:13, 71:18, 73:1, 80:8, 81:19, 85:3 md5 61:8 mean 11:8, 16:11, 16:22, 17:3, 18:2, 24:14, 25:15, 27:14, 32:1, 36:17, 38:3, 38:21, 40:5, 40:16,	40:22, 43:2, 46:6, 46:8, 46:9, 47:22, 49:21, 50:8, 51:5, 60:18, 62:8, 62:22, 71:2, 77:9, 78:13, 80:17, 80:19, 85:13, 89:10, 90:3, 90:16, 92:18, 93:2, 94:12 meaning 25:2, 45:6, 76:2 means 18:5, 34:12, 43:12, 44:3, 67:16, 67:17, 68:2, 76:20, 81:21 meatball 88:3 meet 93:20 members 52:21 mention 52:15, 74:14, 75:9, 78:1, 78:18, 78:20 mentioned 28:19, 66:11, 71:9 metadata 41:18, 42:12, 42:19, 69:8 method 2:11, 62:9 methodology 17:16, 70:8, 82:19 michigan 96:2, 96:21 michigan) 2:9 might 13:3, 22:15,	28:9, 28:15, 30:15, 31:2, 31:17, 65:15, 66:14, 66:15, 78:21, 80:9, 84:1, 85:20 million 67:16 mime 29:17, 29:18 minimum 92:1 minute 74:10, 80:10 minutes 39:11, 39:12 mischaracterizes 21:18, 27:12, 51:7, 58:3, 81:1, 84:21, 89:13, 91:8, 92:16, 93:12 missed 36:10 misstating 88:18 mistakes 8:4 mixed 28:16 mobile 16:22 mode 9:9 modifications 30:6 module 48:10, 49:7 month 78:14 more 13:7, 15:2, 15:4, 15:7, 15:17, 16:3, 16:14, 17:4, 17:22, 21:12, 31:18, 34:5, 37:11, 37:17,	38:4, 38:10, 41:15, 42:9, 42:17, 47:12, 53:11, 53:14, 56:18, 70:13, 80:9, 80:15, 85:19, 87:7, 94:22 most 69:9 move 14:11, 74:13, 79:7, 79:20, 83:10, 84:12, 88:9 movies 69:17 much 8:3, 59:7, 79:15, 87:9 multiple 9:1, 21:15, 21:21, 26:14, 35:1, 56:13, 84:17 must 37:1, 76:12, 78:19, 80:18, 89:11, 89:16, 91:22, 92:14, 92:19, 93:8, 93:18 N name 21:3, 21:15, 21:22, 22:7, 22:13, 22:14, 22:17, 22:19, 23:3, 23:4, 23:7, 23:10, 23:14, 23:15, 24:9, 24:11, 25:1, 27:2, 27:7, 27:21, 28:22, 29:7, 29:12, 30:1, 41:3, 41:9,
--	--	--	--

45:13, 47:8, 55:4, 67:4, 67:8, 71:16, 93:2 names 11:16, 21:10, 21:13, 22:11, 24:10, 24:17, 24:18, 26:3, 27:17, 41:1, 42:11, 42:19, 45:13, 47:10, 52:1, 67:13 namespace 39:16, 39:18, 40:1, 40:3, 40:9, 40:11, 40:14, 41:6, 41:19, 42:7, 42:21, 43:3, 43:8, 43:13, 43:15, 43:21, 44:5, 44:21, 45:3, 45:4, 45:7, 45:8, 45:10, 45:16, 46:1, 46:13, 46:16, 47:7, 47:19, 48:17, 49:11, 49:15, 50:4, 50:12, 50:18, 51:3, 51:4, 51:11, 51:12, 51:14, 51:17, 51:22, 52:3, 52:10, 52:13, 52:18, 52:22, 53:17, 53:22, 54:7, 54:13, 54:14, 55:2, 55:4, 60:20, 66:22, 67:1, 67:2, 67:11, 67:22, 68:3, 68:5 namespaces 21:8, 40:6, 41:17, 42:1,	48:5, 49:3, 50:11, 53:11, 53:14, 85:14 naming 44:19, 49:11 narrative 42:5 narrower 18:20 necessarily 53:18, 81:14, 88:8, 90:2, 90:6 need 7:5, 8:10, 12:6, 12:7, 13:20, 27:19, 30:19, 32:17, 36:18, 45:12, 46:3, 46:8, 46:21, 57:8, 57:10, 57:11, 60:17, 61:22, 65:15, 65:21, 75:9, 78:2, 78:5, 80:9, 81:14, 83:13, 84:16, 84:17 needed 14:6, 26:12 needs 10:5, 13:6, 23:5, 25:12, 26:7, 27:10, 73:14 neither 76:22 netskope 1:6, 5:18 never 25:17, 26:1, 78:11, 79:2 new 14:4, 14:15, 17:16 next 49:9 nice 31:22	nobody 68:7 non-text 71:5 non-zero 75:22 normally 23:17, 29:5 notary 96:1, 96:21 notes 96:12 nothing 6:3, 6:7, 15:18, 33:5, 42:20 notice 8:3 noticed 7:18 notion 18:13 novel 34:22 number 22:4, 35:3, 35:6, 36:7, 64:3, 67:17, 67:20, 81:22 numbered 2:6 numbers 45:20, 46:13, 46:14, 67:15, 72:2 numeral 72:4 O oakland 96:4, 96:21 oath 5:6 obfuscate 61:5 objection 5:20, 9:13, 10:19, 15:11,	16:12, 17:2, 17:17, 18:8, 20:9, 21:4, 21:17, 22:6, 22:21, 23:16, 24:13, 27:12, 29:4, 30:9, 31:15, 33:4, 33:10, 35:13, 40:21, 43:1, 43:18, 49:19, 51:7, 54:1, 54:9, 55:3, 55:10, 56:12, 58:2, 59:3, 61:13, 62:2, 62:21, 63:14, 64:16, 65:13, 67:6, 68:17, 69:6, 74:5, 74:22, 80:22, 82:10, 83:2, 84:20, 85:1, 87:19, 89:13, 89:18, 91:8, 92:16, 93:12 objections 5:11, 5:15, 5:18 objects 47:4 obscure 61:15 obscurity 33:19 obtain 24:12 obviously 57:5, 65:18, 67:15, 82:16, 83:11, 84:6, 93:2 occur 59:13, 77:2, 77:13, 81:9 occurs 76:8 offered 4:15
--	--	--	--

office 1:1 oh 13:18, 72:17 okay 7:12, 8:5, 8:11, 8:21, 8:22, 9:5, 9:19, 10:12, 12:4, 12:6, 14:5, 15:9, 16:20, 17:9, 17:15, 17:22, 18:17, 19:2, 19:6, 19:9, 20:1, 20:19, 22:2, 24:9, 25:8, 26:9, 32:12, 32:16, 34:18, 34:19, 34:20, 37:21, 39:4, 39:21, 40:11, 40:18, 41:5, 41:11, 42:8, 44:17, 45:2, 47:5, 48:14, 48:19, 52:15, 53:3, 55:1, 56:8, 60:6, 60:16, 61:8, 62:12, 63:8, 64:12, 66:20, 70:18, 71:6, 71:17, 71:18, 71:22, 72:8, 72:16, 73:8, 73:9, 74:9, 74:11, 74:12, 76:17, 77:18, 79:6, 79:9, 79:21, 79:22, 80:5, 80:8, 80:11, 82:3, 82:19, 83:9, 83:17, 84:6, 88:9, 88:11, 88:15, 88:16, 89:10, 90:12,	94:22 once 16:17, 50:12, 75:1, 88:3 one 7:19, 8:1, 8:7, 9:7, 14:17, 15:2, 15:4, 15:7, 15:17, 16:3, 16:14, 17:4, 19:20, 20:15, 21:12, 21:19, 27:18, 28:13, 28:15, 28:16, 31:14, 33:12, 34:21, 35:3, 35:10, 37:7, 37:11, 37:17, 38:4, 38:10, 39:6, 41:15, 42:9, 42:17, 44:5, 45:9, 46:5, 46:6, 53:5, 53:11, 53:13, 53:14, 58:21, 63:22, 64:6, 66:4, 72:11, 72:12, 72:13, 72:16, 73:11, 73:19, 73:20, 74:11, 91:16, 92:7, 94:4 one-way 61:1 ongoing 60:9 only 10:1, 13:1, 38:19, 41:7, 41:8, 47:15, 57:9, 59:15, 60:4, 69:21, 70:17, 73:12, 74:2, 75:16, 75:21, 76:13, 76:15, 77:8, 79:1, 85:22	operation 61:19 operations 60:8 operator 88:6 opinion 31:12, 77:11, 77:22 opportunity 7:16 opposed 35:16 option 13:16 optional 75:3, 75:6 optionally 57:16 options 31:11, 88:7 order 18:15, 93:20 ordinary 40:12, 62:17 other 10:4, 10:16, 12:20, 14:17, 22:19, 22:20, 23:4, 23:7, 25:13, 31:1, 34:9, 36:15, 40:3, 40:20, 47:20, 49:17, 64:1, 69:17, 70:22, 75:18, 76:7, 90:17, 91:19 otherwise 25:7 out 7:21, 8:7, 26:17, 39:19, 43:10, 44:2, 62:15, 63:9, 63:18, 70:2, 86:18, 87:10, 91:19	output 29:6, 31:8, 31:9, 65:22, 66:3, 66:12, 68:9 outputs 25:17, 25:19, 65:1, 68:1, 68:6, 68:7, 68:8 outputting 54:10 outside 38:19, 91:5 over 13:19, 14:3, 35:1, 79:10 overlap 9:16 own 50:5, 58:6 owner 1:10, 3:14, 5:20 P page 4:3, 4:13, 19:7, 32:3, 71:22, 72:1, 72:2, 72:11, 73:6, 76:10, 76:11, 79:20 pages 1:20 pair 33:14 paper 20:11, 20:17, 71:11, 81:4, 84:2, 84:4, 84:6, 88:7 papers 18:11 paragraph 8:12, 8:15, 9:6, 19:6, 19:8, 19:11, 31:22, 32:1, 34:19,
--	--	--	--

34:21, 36:9, 36:10, 38:16, 44:14, 44:17, 48:3, 48:4, 48:19, 50:3, 50:7, 55:15, 55:16, 76:2, 77:12, 77:15, 77:17, 78:17, 79:22, 80:6, 83:22, 88:10, 88:12, 88:14, 89:3, 89:19, 92:14, 94:7 paragraphs 19:2 parameters 18:22 parse 24:11 parses 24:18 part 6:17, 7:19, 19:10, 20:8, 21:3, 27:10, 28:15, 28:16, 32:2, 38:7, 43:8, 43:12, 43:19, 43:22, 44:12, 45:9, 47:15, 48:5, 49:3, 49:22, 51:21, 52:19, 53:16, 54:12, 61:22, 69:9, 71:10, 76:21, 77:14, 80:11, 80:20, 83:11, 84:7, 88:4, 90:22, 92:14, 93:9 participants 44:5 participating 5:4 particular 12:12, 23:11,	27:19 parties 5:10, 58:18 parts 93:17 party 57:20, 58:10, 96:14 passage 42:7 patent 1:1, 1:4, 1:10, 1:13, 3:14, 5:19, 7:21, 8:17, 9:3, 17:11, 17:13, 17:20, 18:18, 19:17, 20:6, 20:11, 20:12, 31:13, 32:5, 32:19, 35:20, 36:14, 36:19, 37:3, 37:8, 39:17, 40:6, 41:5, 45:16, 48:4, 48:8, 48:15, 49:2, 49:14, 51:2, 52:11, 54:18, 55:17, 55:20, 55:21, 55:22, 57:2, 60:3, 63:19, 67:3, 68:15, 71:5, 84:7, 84:8, 84:13, 85:1, 85:12, 85:13, 91:13, 94:12 patent's 43:13 patents 56:5 path 46:8 pdfs 69:15 penalty 5:8	pending 92:11, 92:13 perfect 79:13 perform 18:14, 35:8, 35:10, 35:14, 36:21, 38:21, 39:1 performed 35:4, 88:1 performing 56:10, 56:21 perhaps 11:2, 30:16, 47:15, 50:16 perjury 5:9 perkins 3:6 person 5:7, 11:5, 12:5, 40:12, 44:7, 60:4, 62:16, 82:15 persons 44:7 perspective 18:4, 40:12, 62:16 petition 70:9 petitioner 1:7, 2:5, 3:3, 5:18 petitioner's 70:10 ph 1:15, 2:4, 3:5, 4:4, 5:1, 5:6, 6:4 phrase 86:10 pick 30:12 piece 24:18 pieces 12:2	place 14:15, 44:2, 47:2, 79:5, 87:17 placed 86:1 places 29:15, 36:15, 47:16 plaintext 7:20, 12:16, 32:17, 33:9, 33:13, 33:22, 34:12, 64:4, 65:3, 66:7, 77:10, 78:11, 78:12, 79:2 plaintexts 34:13 planet 46:3 platform 51:18 platforms 15:4, 51:19 plays 50:17 please 5:14, 5:21, 7:2, 7:6, 19:3, 39:8, 44:15, 46:11, 88:12, 92:8 plurality 53:10, 53:12 point 39:21, 41:11, 42:1, 53:1, 60:6, 65:6, 73:1, 78:4 pointed 92:5 pointer 90:5 policies 12:12, 15:5, 15:20, 17:4, 17:7, 48:11,
--	--	--	---

49:10, 50:13, 53:4 policy 8:22, 9:20, 10:1, 10:5, 10:9, 10:12, 10:13, 10:14, 10:17, 10:21, 12:1, 12:8, 12:9, 12:13, 13:3, 13:5, 13:12, 14:1, 14:6, 14:10, 14:13, 14:17, 14:18, 14:19, 15:1, 15:2, 15:15, 16:1, 16:6, 16:10, 16:20, 43:19, 43:20, 43:22, 44:8, 50:16, 51:2, 51:4, 51:13, 51:15, 51:16, 52:2, 52:4, 52:7, 52:9, 52:12, 88:21, 89:2, 91:7, 91:11, 91:17, 92:19 portions 18:12, 86:21 posita 40:15, 51:12, 89:4, 89:20, 93:15 position 70:6 positive 82:9 possible 34:2, 41:8, 45:6, 46:17, 54:12, 54:13, 58:4, 58:5, 67:4, 67:10, 68:1, 68:5, 68:7, 68:8, 80:1, 94:7	possibly 60:1 potentially 66:5 power 38:13, 39:2, 59:7 powerful 35:4 practice 17:5 preselect 86:4 present 29:2 presumably 56:22 pretty 21:19 prevention 74:15, 75:3, 78:2 print 29:9 printable 29:20 prior 17:13, 35:1, 73:5, 75:13, 75:14, 84:22 private 48:9, 49:6, 52:16, 55:18, 56:1, 56:3, 56:6, 56:16, 57:1, 57:4, 57:7, 57:17, 57:20, 58:1, 58:6, 58:16, 72:21, 75:20 probably 17:14, 30:11, 30:19, 34:5, 43:5, 70:18, 78:14, 81:15, 90:18 procedure 2:12, 56:9	proceed 6:11 proceeding 5:15 proceedings 95:2 process 9:20, 10:2, 10:9, 10:11, 14:5, 29:19, 34:22, 48:6, 49:4, 54:10 processed 10:7 processing 9:8, 10:14, 15:3, 72:19 produce 53:21, 61:9, 64:18, 66:3, 68:20, 82:9 produced 2:4, 64:13, 80:14 produces 33:1, 65:10, 65:22 producing 68:14 professional 83:5 prohibit 16:9, 16:16 prong 80:12, 83:10 property 76:13 proscription 23:7 provide 46:10, 61:12 provided 75:20 provider 27:17, 27:18, 38:20, 43:3, 43:5, 43:10, 44:4, 47:6,	57:22, 59:21, 60:5, 61:11, 61:12, 72:20, 73:11, 73:14, 73:22, 74:18, 74:20, 75:15, 75:20, 76:22, 77:3, 77:7, 78:6, 79:1, 79:4, 83:19 provider's 47:8, 85:9 providers 41:17, 42:4, 42:11, 44:10, 58:13 provides 34:22, 48:4, 49:2, 50:3 providing 18:18, 41:11 provisions 2:13 ptab 1:12 public 35:9, 35:12, 36:1, 36:11, 36:13, 36:17, 36:18, 48:9, 49:6, 52:16, 55:18, 56:1, 56:2, 56:5, 56:15, 57:6, 57:14, 57:18, 57:21, 58:8, 75:12, 96:21 public-key 35:15, 36:2, 36:5, 36:20, 55:7, 55:12, 56:9, 59:6 punctuation 30:19 pursuant 2:12 push 30:21
--	---	--	--

put 21:12, 22:12, 23:13, 28:14, 44:3, 47:17, 66:13 putting 20:3, 26:3	88:13, 92:8, 92:11, 92:13, 93:6, 94:4 questions 7:3, 32:2, 39:6, 52:5, 88:22, 94:2, 94:22, 96:9 quickly 24:17 quincy 3:15, 5:19 quincylu@quinnem- anuel 3:21 quinn 3:16 quite 46:9 quote 91:12 quotes 81:18 quoting 55:20	55:5, 64:9, 67:4, 67:8, 67:18, 67:19, 67:21 rdr 1:22, 2:8, 96:20 re-encrypted 14:4 re-encrypting 13:21 read 8:16, 8:19, 8:21, 9:21, 11:1, 15:16, 19:7, 35:21, 42:7, 44:17, 49:10, 52:11, 62:8, 71:13, 73:4, 73:8, 75:1, 75:8, 77:12, 78:13, 78:14, 78:17, 78:18, 78:19, 80:9, 81:3, 81:8, 88:12, 88:15, 88:17, 90:8, 91:13, 97:5 readable 12:20 reading 17:13, 40:5, 41:13, 56:7, 62:7, 75:4, 78:15, 80:5, 93:10 ready 71:3 real 3:7 realize 45:2 really 12:22, 13:3, 30:22, 46:1, 65:6, 70:9, 70:11, 81:10,	84:4 reask 85:3 reason 7:5, 77:20 reasonable 66:8 reasons 64:20 recall 15:18, 31:19, 37:5, 37:6, 39:20, 69:20, 71:4, 84:2 receive 29:16 received 72:19, 73:13, 74:3, 75:17, 77:9 recently 81:4 recited 56:5 recites 14:18 reconstitute 57:19 reconstituting 58:17 record 2:13, 6:17, 7:5, 39:13, 39:14, 74:18, 74:21, 75:10, 76:19, 76:21, 77:1, 77:6, 78:9, 79:16, 79:17, 93:5 record-by-record 76:4, 77:5 recorded 96:10 records 72:20, 73:12, 74:2, 74:16, 75:16, 75:21, 75:22, 76:13,
Q	R		
queries 19:14, 20:3, 81:6, 84:3 query 25:4, 26:9, 26:10, 27:9, 27:11, 28:5, 28:6, 35:8, 35:11, 36:18, 58:11, 61:11, 65:11, 72:13, 72:16, 72:19, 73:2, 73:9, 73:13, 74:3, 74:11, 75:17, 76:12, 76:16, 77:9, 80:11, 80:13, 80:21, 81:14, 82:9, 83:13, 83:20, 84:12 question 8:20, 13:13, 14:17, 14:22, 15:5, 21:11, 32:12, 33:12, 33:20, 35:10, 35:14, 36:3, 36:4, 38:7, 44:18, 48:18, 49:13, 49:20, 50:10, 56:8, 70:12, 70:19, 71:2, 71:9, 78:7, 79:6, 80:6, 80:8, 82:2, 82:19, 85:1, 85:2, 86:9, 88:2,	race 80:1, 80:12, 80:13, 81:15, 83:13, 85:7, 86:16, 86:22, 87:5 raise 5:22 raised 70:10 random 64:3 randomness 64:21 range 40:16, 40:18, 40:19, 45:6, 45:12, 45:13, 47:10, 47:21,		

76:15, 77:8, 77:9, 81:7, 81:8, 81:10, 81:12, 86:19, 86:21 red 85:22, 86:3, 86:7, 86:10 redirect 94:3 reduce 66:5 reduced 96:10 reduces 66:5 refer 6:18, 19:8, 41:19 reference 84:22 referred 19:12 referring 41:20 refill 39:10 reflect 13:12, 14:10 regarding 84:21, 92:9 related 11:14, 96:13 relatively 66:16 relevant 71:8, 76:15 remember 71:14, 71:15, 72:9, 88:17 remit 58:13 remote 14:9 remove 14:8 render 65:15	repeat 67:7 repeats 9:10 rephrase 20:5, 36:3, 68:19 replace 13:15 report 32:11 reported 1:21, 2:11 reporting 5:12 repositories 11:18, 14:13, 21:8, 21:9 repository 14:12 reproduced 32:4 require 23:2, 36:20, 60:18 required 55:9, 55:13, 67:3, 67:10 requirement 77:17, 78:22 requirements 92:2 requires 17:3, 18:21, 54:11, 60:19, 78:8, 84:11 reserved 26:4 reside 14:16, 47:9 respect 29:20 respond 70:9 rest 46:3, 78:3 restrict 31:13	restrictions 11:12, 31:18 result 28:17, 75:18, 75:22, 76:11, 82:9, 82:13 results 86:16, 86:17, 87:1, 87:2, 87:16 retrieve 57:11, 73:11, 74:1, 75:16, 77:7 return 25:6, 75:22, 76:15 returned 76:12, 87:1 returning 86:19, 86:20, 86:21 reverse 33:8, 33:12, 61:2, 68:4 review 72:9 right 5:22, 7:8, 7:10, 8:12, 10:8, 10:22, 11:2, 15:7, 16:4, 16:16, 18:20, 20:20, 24:14, 25:5, 29:5, 46:20, 47:12, 49:4, 50:2, 54:4, 55:18, 55:21, 57:5, 58:19, 60:6, 60:19, 61:3, 68:4, 69:11, 74:4, 75:19, 76:5, 86:19, 91:7, 92:1, 92:4, 94:18, 95:1 rights 10:8, 10:22,	11:3, 11:9, 12:6, 12:17, 12:19 rmr 1:22, 2:8, 96:20 roman 72:4 ronn 7:22, 32:6, 32:12, 63:20 rpr 1:22, 2:8, 96:20 rules 2:12, 29:21, 30:4, 30:20 rxw 12:18 S s 17:14 s3 11:16 safe 14:7 said 7:19, 9:16, 28:17, 34:16, 39:21, 40:18, 46:19, 60:2, 62:6, 67:15, 71:14, 82:7, 82:21, 84:13, 85:18, 92:7, 93:15, 94:18 salt 74:17 same 19:7, 24:6, 32:17, 34:14, 38:11, 55:1, 57:20, 63:22, 64:5, 64:9, 64:10, 64:13, 64:14, 64:19, 64:22, 65:3,
--	---	--	---

65:9, 65:11, 65:16, 65:22, 66:3, 69:3, 73:6, 94:7, 97:6 san 3:9 satisfied 81:15 satisfy 16:2, 38:6 saw 40:2, 63:19 say 10:10, 11:1, 12:17, 13:7, 13:9, 13:17, 13:22, 14:1, 14:13, 15:22, 16:11, 16:14, 19:17, 23:12, 23:21, 24:14, 24:21, 25:2, 25:7, 25:10, 25:12, 29:5, 29:22, 30:21, 32:11, 33:20, 35:3, 35:22, 36:21, 39:11, 40:22, 41:8, 41:9, 43:2, 43:10, 44:6, 45:2, 45:11, 45:19, 46:5, 46:12, 46:20, 48:4, 48:7, 48:21, 49:5, 50:19, 51:1, 51:16, 55:16, 58:6, 59:12, 61:3, 67:18, 67:22, 68:2, 68:5, 69:11, 71:4, 80:17, 80:18, 83:12, 83:22, 86:2, 86:7, 86:22, 89:4, 89:19, 91:16, 92:18,	93:17 saying 12:14, 13:13, 25:8, 36:12, 36:14, 36:16, 41:14, 49:1, 50:6, 50:9, 51:10, 53:7, 54:15, 55:12, 57:21, 58:19, 60:16, 62:4, 75:19, 76:7, 77:16, 78:13, 81:5, 82:1, 83:4, 87:13, 90:4, 94:12, 94:14 says 8:22, 9:22, 10:21, 13:18, 15:1, 15:17, 19:11, 21:20, 25:5, 31:19, 32:9, 34:22, 37:10, 37:15, 38:3, 38:7, 38:9, 38:16, 39:22, 42:21, 44:18, 49:10, 49:14, 51:2, 52:8, 53:1, 53:9, 54:3, 55:22, 61:20, 69:21, 69:22, 72:5, 72:16, 74:6, 74:14, 75:2, 75:14, 75:15, 77:7, 80:1, 80:13, 80:19, 81:7, 82:12, 83:11, 85:13, 88:17, 88:18, 88:19, 91:12, 91:14, 93:7 scenario 26:9, 28:5, 38:18, 73:22	scheduling 5:16 scheme 13:11, 17:16, 18:18, 18:22, 19:18, 20:3, 22:5, 31:3, 72:17, 72:19, 75:7 schemes 31:7 science 12:15, 40:14, 48:1 scope 16:13, 17:2, 22:22, 44:21, 45:3, 45:5, 45:8, 45:11, 46:16, 54:13, 56:4, 70:18, 91:5, 94:8, 94:20 scratch 22:2, 77:19, 90:14 search 11:21, 11:22, 17:18, 18:6, 18:14, 18:15, 19:13, 19:14, 19:18, 20:3, 20:7, 20:22, 21:2, 21:15, 21:21, 22:4, 22:20, 23:9, 23:12, 23:13, 23:14, 23:22, 24:2, 24:10, 24:12, 24:22, 25:3, 25:10, 25:14, 26:9, 26:10, 27:9, 27:11, 28:4, 28:6, 29:1, 30:7, 31:6, 32:5, 33:14, 35:3, 35:6,	35:14, 38:12, 38:21, 39:1, 60:12, 60:14, 60:21, 61:2, 61:5, 61:7, 61:10, 61:16, 65:8, 65:10, 65:11, 65:12, 65:16, 66:10, 66:14, 66:16, 69:10, 69:13, 76:5, 76:6, 80:1, 80:7, 80:21, 81:16, 82:13, 82:19, 83:1, 83:17, 83:20, 84:14, 84:16, 84:17, 84:18, 85:3, 85:6, 85:8, 85:10, 86:4, 86:6, 86:15, 87:2, 87:11, 87:16, 87:18, 88:6 searchable 17:13, 17:15, 18:1, 18:5, 18:19, 18:21, 23:3, 23:6, 26:21, 37:12, 37:16, 37:22, 38:5, 38:10, 42:13, 53:15, 68:14, 68:21, 69:8, 69:22, 70:7, 72:5, 72:17, 72:18, 85:15, 86:13 searched 9:9, 12:1, 38:1, 69:15, 85:21 searches 37:4 searching 11:20, 18:12, 24:9, 34:14,
--	--	---	---

77:6, 82:20, 86:15 seattle 3:19 second 28:16, 32:2, 50:21, 53:5, 53:11, 74:19, 75:7, 77:2, 77:13, 80:11, 83:10 secret 48:9, 55:18, 73:15, 74:1 secretly 68:10 section 10:13, 10:14, 10:15, 10:17, 72:4, 72:8, 73:9, 74:11, 78:14, 79:20, 79:22, 80:6 sections 6:16, 12:2 security 10:22, 11:5, 33:18 see 19:15, 23:6, 25:12, 32:7, 32:14, 34:13, 36:10, 37:13, 37:19, 42:15, 42:16, 42:20, 44:22, 48:12, 51:5, 51:6, 51:10, 52:19, 55:19, 57:9, 67:15, 70:10, 72:3, 72:6, 72:7, 72:14, 72:15, 74:6, 74:18, 74:21, 75:2, 77:6, 79:13, 80:3, 81:8, 89:8 seeing 9:6, 37:5,	73:17 seem 75:5, 79:2 seems 61:19, 73:9, 77:21, 81:5 seen 18:9, 18:10, 41:15, 42:9 segue 31:22 select 85:20 selected 91:17 send 29:16, 30:3, 57:3, 76:3, 76:8, 76:21 sending 27:9 sense 18:20, 34:7, 43:13, 69:20, 70:2, 87:9 sensitive 31:2 sent 72:22, 83:18, 88:3 sentence 8:17, 8:21, 8:22, 9:2, 9:5, 19:10, 34:22, 35:21, 44:18, 49:1, 49:9, 74:13, 75:13, 75:14, 76:11, 77:16, 78:3, 78:8, 78:18, 81:8, 89:3, 92:13, 93:6, 93:11 separate 9:11, 11:10, 24:17, 24:22, 28:18, 65:18 separated 45:21	separately 84:17, 85:10 separator 23:18, 24:1 sequentially 86:15 serve 61:5, 61:15 server 14:9 service 24:19, 26:20, 30:3, 31:3, 35:4, 38:17, 41:17, 42:4, 42:11, 60:5, 61:11 set 12:15, 39:6, 39:19, 40:22, 58:4, 60:2, 64:21, 65:17, 67:12, 67:13, 96:8 setup 72:11 several 53:6, 87:21 sha 61:9, 68:9 sha-1 66:11, 66:12, 66:15, 68:1, 68:4, 68:13 share 58:7, 78:5 shazam 70:16, 70:19 sheet 97:8 short 19:6, 24:4, 88:13, 94:4 shorter 66:14 should 7:22, 74:15, 85:3, 93:14	shouldn't 88:14 show 37:2, 65:2, 80:20 showing 41:14, 42:4 shown 13:14 shows 39:22, 42:17 shrink 66:9 shrinking 66:19 sign 83:12 signature 97:17 signature-k9lvk 96:18 signed 97:8 silly 57:12, 79:2 similar 14:5, 83:12 simply 94:8 simultaneous 67:5 since 58:15, 60:2, 66:16, 81:20 single 15:15, 21:22, 59:15, 72:21, 86:3 sitting 70:14 six 9:6, 9:11, 9:17, 32:20, 32:21, 33:2, 63:20 six-letter 32:13 size 34:3, 63:11,
--	---	---	---

63:12, 63:13, 63:18, 66:5, 66:6, 66:10 skill 40:12, 62:17 slash 29:22, 30:2 slashes 30:22 small 66:10, 66:16 smaller 66:6 software 12:9, 24:18 solely 83:7 some 6:15, 6:16, 9:16, 11:4, 12:21, 12:22, 17:10, 22:8, 27:22, 29:10, 29:19, 43:9, 60:14, 60:16, 64:18, 67:13, 70:1, 71:13, 73:3, 78:21, 82:8, 82:14, 85:18, 86:8, 86:16, 88:6, 90:7, 94:19 somebody 13:6, 24:9 somehow 24:11, 68:13 someone 12:4 something 9:14, 11:17, 12:18, 13:5, 23:21, 24:5, 25:21, 29:1, 29:20, 30:15, 43:4, 48:22, 67:14, 69:19, 82:12, 92:20 sometime 80:5	sometimes 12:15, 57:2, 60:3 somewhere 31:17, 84:1 sorry 16:12, 48:18, 55:12, 56:18, 56:20, 72:18, 78:10 sort 12:21, 15:14, 58:9, 64:8 sound 69:11, 69:18 sounds 7:7, 57:12 space 22:7, 23:3, 34:3, 41:9, 44:10, 46:22, 47:1, 64:10, 86:10 spaces 23:5 speaking 67:5 speaks 21:5 spec 7:21 special 26:4, 30:14 specific 13:8, 20:6, 20:16, 22:9, 56:2, 56:19, 80:7, 80:15, 83:16, 85:12, 87:11 specifically 31:20, 60:12, 80:18 specification 15:18 specify 46:8, 47:7, 91:4	spend 70:11, 80:5 ss 96:3 standard 11:4 start 7:13, 26:15, 52:6, 63:1, 71:18, 73:19 starting 5:16, 52:3 starts 8:17, 25:11, 28:14, 50:13, 62:3 state 5:14, 96:2 stated 2:13, 43:20, 50:10 statement 50:2, 66:8, 92:4 states 1:1 stay 30:18 stenographer 5:4, 5:21, 6:10, 67:7 stenographic 2:11, 96:12 stenographically 1:21, 96:10 step 37:10, 39:3, 50:17, 62:8, 72:17, 72:18, 73:2, 73:6 steps 25:13, 53:6, 56:10, 72:10, 73:5 still 36:7, 38:10, 38:11, 38:21, 66:22, 75:22	stipulate 36:22 stipulates 36:11 storage 11:18, 12:12, 14:6, 14:12, 26:11, 26:13, 26:17, 27:10, 29:21, 30:8, 40:3, 43:11, 43:16, 47:6, 47:8, 47:9, 52:7, 57:21, 57:22, 59:14, 59:21, 79:3, 83:18, 85:9 store 19:18, 27:1, 38:18, 38:19, 41:18, 42:12, 42:19, 47:6 stored 9:9, 10:2, 11:15, 12:7, 12:10, 15:3, 19:14, 50:14 storing 10:15, 14:9, 44:20 story 43:22, 44:4, 44:13, 50:13, 60:4 string 27:21, 68:9 strong 33:2, 33:5 study 84:4 stuff 28:2, 78:21 sub-limitation 53:9 subject 70:7 submit 34:13
---	--	---	--

submitted 18:11 substance 8:6 substantive 7:14, 8:9 subsystems 62:9 suite 3:8, 3:18 sullivan 3:16 supplemental 6:19 suppose 17:5, 34:16, 38:11, 38:21, 77:4, 87:8 supposed 51:19, 52:1 sure 7:2, 10:10, 14:21, 16:17, 21:19, 25:16, 28:18, 29:2, 30:3, 46:12, 48:18, 50:22, 53:2, 70:12, 73:7, 73:17, 81:4, 82:1, 94:4 swear 6:1 switch 17:9, 66:21 sworn 2:5, 6:6 symmetric 36:15, 53:20, 54:6, 59:12, 59:20, 74:16, 90:18 symmetric-key 35:16 system 15:22, 16:1, 20:16, 22:11, 22:14, 24:20, 25:4, 25:8,	25:16, 26:6, 26:8, 26:21, 30:4, 30:12, 30:16, 30:20, 43:7, 63:21, 64:4, 65:15, 71:16, 76:15, 78:16, 79:3, 83:3, 83:16, 84:12 systems 11:1, 11:6, 18:10, 29:21, 30:8, 63:16, 64:7 T table 81:16 tables 81:6, 81:12 tagged 82:9 tags 69:8 take 7:5, 21:2, 34:8, 39:7, 53:18, 66:11, 70:1, 73:3, 88:14 taken 2:6, 44:1, 96:7, 96:13 takes 87:17 talk 6:21, 17:10, 39:16, 47:3, 60:3, 72:9, 73:5 talked 63:8, 65:7 talking 22:10, 47:3, 47:13, 65:6, 85:18, 87:22 talks 9:7, 36:14,	42:5, 57:2, 79:22 task 13:21, 58:16 teaches 48:8, 55:17 technique 38:12, 69:4, 78:12 techniques 24:7 technologies 70:16 technology 26:22 tehranchi 3:4, 4:7, 5:17, 6:12, 6:14, 9:18, 16:19, 17:8, 17:21, 18:16, 20:18, 21:14, 22:1, 22:18, 23:8, 24:8, 28:3, 31:21, 33:7, 35:18, 39:5, 39:12, 39:15, 41:4, 43:14, 50:1, 54:2, 54:19, 55:6, 55:14, 56:17, 59:11, 61:18, 62:11, 63:3, 65:5, 67:9, 68:18, 74:8, 79:9, 79:11, 79:14, 79:18, 82:18, 83:8, 85:5, 89:15, 90:11, 91:2, 92:12, 93:3, 93:21, 94:1, 95:1 tell 10:12, 12:5, 12:18, 27:6, 40:8, 46:3, 65:2, 67:20,	68:8, 89:16 telling 68:11 tells 52:13, 88:8, 90:21 ten 39:11, 39:12 ten-minute 39:7 term 18:9, 23:14, 23:20, 23:22, 24:2, 24:6, 24:12, 24:22, 25:3, 25:10, 25:14, 32:5, 40:9, 41:2, 45:16, 61:2, 61:5, 61:16, 65:12, 65:17, 77:4, 84:16, 86:3, 90:9, 91:22, 93:20, 94:8, 94:9, 94:17, 94:20 terminology 70:20 terms 19:13, 19:18, 20:7, 21:1, 21:2, 21:15, 21:21, 22:4, 22:9, 23:10, 23:12, 23:13, 23:19, 29:1, 30:7, 61:10, 64:12, 66:10, 66:14, 69:15, 80:7, 83:17, 83:19, 85:7, 85:10, 87:11 testified 6:8 testify 6:6 testimony 5:8, 6:1,
--	--	--	--

21:18, 27:13, 51:8, 58:3, 97:5, 97:7 text 29:11, 68:16, 68:20, 69:2, 69:16, 69:21, 70:21, 71:1, 80:1, 80:18, 80:19, 81:14 thank 6:10, 6:12, 7:8, 8:11, 14:17, 79:14, 93:22 thanks 79:15 themselves 43:5 theoretically 56:13 therefore 13:15, 16:5, 43:21, 49:10, 49:11, 89:4, 89:20 thereupon 6:5 thing 62:4, 64:5, 64:19, 64:22, 65:4, 65:9, 69:21, 75:9 things 8:3, 8:9, 9:1, 9:17, 10:4, 11:1, 11:14, 12:15, 23:4, 26:8, 26:15, 31:1, 31:11, 40:5, 40:20, 47:2, 47:17, 50:8, 50:14, 54:18, 58:4, 63:1, 69:16, 78:5, 79:5, 89:11, 90:20, 94:10, 94:14,	94:16 think 7:18, 8:2, 8:5, 8:9, 9:2, 9:16, 10:8, 14:18, 15:21, 16:7, 16:8, 19:21, 20:14, 21:19, 23:1, 23:2, 28:11, 31:4, 31:22, 32:4, 32:9, 34:21, 35:20, 36:15, 37:7, 39:19, 40:22, 41:7, 42:1, 42:3, 43:19, 51:11, 52:8, 52:11, 57:13, 58:4, 58:5, 61:6, 62:3, 63:8, 63:16, 63:21, 64:6, 66:11, 68:19, 69:19, 70:19, 71:3, 71:19, 74:7, 74:10, 75:3, 78:8, 78:22, 84:11, 85:4, 87:4, 87:9, 88:2, 88:6, 90:2, 90:3, 90:5, 90:7, 91:21, 93:4, 93:14, 94:14 thinking 69:14, 70:11, 75:5 third 58:9, 79:22 thought 40:2, 70:5, 86:13 thread 85:4 three 23:12, 45:20, 47:11, 56:10,	62:9, 73:5 three-digit 46:13, 46:14 through 6:15, 6:21, 24:16, 24:20, 41:7, 71:17, 73:5, 73:8 throw 51:17 time 2:7, 34:8, 39:7, 57:7, 57:9, 64:2, 64:5, 64:19, 70:1, 70:11, 73:3, 79:10, 79:12 time-consuming 59:1 times 12:20, 57:4 today 6:15 together 28:14, 84:18, 85:11, 86:3, 87:13 token 72:12 told 45:20, 46:21 took 66:17 top 76:10, 91:15 totally 8:10 trademark 1:1 transcript 5:13, 96:12 transcription 96:11, 97:7 transformation 61:4 transitive 16:4	trial 1:4 trivial 34:4 true 32:15, 32:18, 48:22, 96:11, 97:6 trusted 72:21, 74:15 truth 6:2, 6:3, 6:6, 6:7 try 29:8, 34:1, 34:9, 61:1, 64:19, 87:7 trying 18:3, 34:2, 34:7, 62:15, 63:16, 66:7, 70:9, 76:9, 76:14, 87:10 turn 75:6, 82:13 turned 66:17 twice 63:22, 64:13, 64:22 two 25:6, 35:6, 38:15, 54:17, 60:8, 65:1, 65:2, 73:10, 73:18, 78:15, 81:9, 82:17, 85:3, 85:6, 87:11, 87:13, 89:11 type 31:14, 34:15, 89:7, 89:12, 90:1, 90:13, 90:16, 90:22, 91:5, 91:18, 93:1, 93:7, 93:9, 93:20,
--	--	--	--

94:11 types 35:20 typical 10:22, 81:16, 90:19 typically 18:10, 19:13, 29:9, 29:17, 41:1, 66:9, 68:12 typo 32:19 typographical 7:18 typos 7:14, 8:8	undesirable 59:8, 65:14 unique 74:16 united 1:1 universe 45:22 unless 16:15, 52:6, 68:10, 86:13 update 13:22, 14:13 upper 30:17 urquhart 3:16 use 13:11, 14:2, 19:17, 19:18, 20:7, 23:18, 24:19, 26:4, 29:7, 29:17, 29:18, 30:17, 31:7, 35:15, 35:22, 36:2, 36:5, 36:6, 38:11, 51:20, 65:21, 66:1, 86:11 user 11:9, 11:19, 11:21, 14:1, 14:14, 14:18, 14:19, 15:6, 15:8, 16:21, 35:5, 43:17, 57:3, 57:4, 58:6, 58:21, 60:2, 76:3, 76:12 user-assigned 48:11 users 10:1, 10:2, 15:2, 15:9, 15:10, 15:17, 15:19, 16:1,	16:2, 16:3, 16:5, 16:6, 16:10, 16:14, 16:22, 17:1, 17:4, 17:7, 37:11, 37:17, 38:4, 38:10, 53:4, 60:4 uses 40:9, 45:16 using 24:22, 27:19, 29:5, 31:4, 35:9, 35:12, 36:13, 36:14, 36:17, 36:20, 37:17, 47:5, 48:15, 53:20, 56:8, 58:8, 59:19, 61:16, 63:5, 65:20, 74:16, 88:20, 91:10 usually 33:16, 63:17, 64:1, 66:6	87:19 valid 27:16 value 67:20 values 22:9, 40:17, 40:18, 41:1, 45:6, 45:12, 46:4, 46:17, 47:10, 47:21, 55:5, 64:12, 65:11, 67:4, 67:11, 67:13, 67:15 variable 31:9, 31:19, 63:10, 64:5 variant 73:18, 73:19, 74:9, 75:7 variants 73:18, 74:7 variation 74:20, 75:1 variations 73:10 various 21:7, 21:9, 21:13, 24:7, 44:10, 47:16 vendors 11:16, 31:1 verbatim 82:6, 82:16, 82:20, 83:1, 83:14 verified 5:5 versus 16:22, 31:19 vertical 23:21, 24:22, 25:3, 25:6, 25:18, 25:22, 26:4, 27:5, 27:6, 27:7 via 2:11, 67:13,
U		V	
uetywo 32:7, 32:13 unclear 7:2, 66:22 under 5:8, 11:2, 13:21, 14:4, 56:11, 57:5, 57:14, 61:6, 79:22 understand 6:20, 13:2, 13:4, 13:13, 28:4, 47:3, 48:18, 51:12, 58:10, 58:14, 60:9, 68:1, 80:9, 87:17, 89:4, 89:20 understanding 18:3, 40:11, 51:11, 62:14, 80:14 understands 11:22 understood 7:1, 36:19, 40:16, 93:16 undertake 13:20, 58:16			

96:8 video 70:22 videoconference 2:11, 96:8 view 18:17, 45:14, 45:15, 84:10 virtually 22:10 visually 5:7 vs 1:8	19:20, 20:15, 23:17, 25:15, 26:2, 28:8, 29:10, 30:1, 33:13, 40:4, 41:8, 45:16, 51:14, 58:5, 60:2, 62:7, 65:1, 75:4, 75:8, 77:12, 82:1, 84:19, 85:12, 85:15 ways 11:7, 18:10, 34:9, 56:13, 81:13, 82:5, 83:6, 87:21 we'll 60:6, 71:18 we're 13:7, 19:7, 22:10, 24:15, 26:19, 47:3, 47:13, 56:8, 62:7, 69:22, 73:6, 79:10, 86:18, 87:22, 91:21, 95:1 web 29:18 webster 1:22, 2:8, 96:6, 96:20 wednesday 1:16, 5:2 week 20:15 wei 3:5 whatever 29:21, 61:8, 63:5 wherein 37:16 whether 12:4, 15:21, 67:20, 68:9, 69:20, 70:2,	70:6, 88:1, 88:2, 90:17 whoever 14:15, 50:16 whole 6:3, 6:7, 11:6, 11:7, 76:11, 88:2 wild 26:8 windows 46:19 windows-based 30:16 within 45:12, 46:14, 47:4, 47:9, 47:21, 55:4, 55:5, 67:18, 67:19, 84:22, 86:21, 94:16, 94:20 without 18:6, 18:14, 26:17, 40:9, 47:19, 52:3, 57:6, 61:16, 68:11, 68:12 witness 2:5, 4:3, 5:5, 5:7, 6:5, 6:9, 39:10, 79:9, 79:13, 79:15 word 10:11, 24:4, 32:13, 57:10, 69:15, 71:15, 81:20, 82:17, 83:1, 83:7, 86:6, 86:7, 87:18 words 20:20, 49:17, 50:5, 60:12, 60:15, 65:8, 65:10, 66:16, 76:7, 82:17, 82:20, 83:13,	84:12, 84:14, 84:18, 85:3, 90:17 work 29:15, 53:21, 54:6, 55:8, 61:17, 70:14, 77:18, 79:12, 81:11, 87:8 works 59:16, 78:17 world 45:22 worry 30:19 wouldn't 30:13, 30:14, 38:12, 48:2, 57:9, 59:1, 65:19, 66:4, 82:16, 86:12, 93:17 write 7:17 writes 52:12 writing 50:13, 83:7 wrong 7:19, 7:20, 7:21, 18:3, 28:9, 28:17, 28:20, 32:10, 48:20, 60:10, 93:11 wrote 44:7, 67:17, 93:14 wyuan@perkinscoie 3:12
W			
waive 5:11 walk 6:15 want 8:7, 13:10, 14:8, 18:13, 20:19, 28:17, 29:16, 30:22, 39:9, 48:21, 57:10, 58:7, 59:8, 59:10, 73:3, 76:19, 78:21, 80:8, 82:21, 85:2, 85:8, 86:3, 87:17 wanted 6:17, 30:21, 69:13 wants 81:8 washington 2:10, 3:19 waste 57:7 water 39:11 watermarking 70:13 way 15:15, 16:4,			
X			
xml 12:21 xyz 78:19			
Y			
yeah 9:14, 20:19,			

26:19, 28:8, 31:11, 44:17, 47:12, 60:18, 70:9, 73:7, 82:12, 87:21, 88:12, 93:4 yourself 58:17, 87:1 yuan 3:5 z zero 76:2, 76:20, 79:1 . .5734 3:10 .7000 3:20 0 00458 1:12 039 30:18 06 1:17, 2:7 07 39:14 084.004953 2:10 1 10 41:13, 42:8 1001 37:8, 71:12, 71:20, 79:20 11 41:13, 42:8 1109 3:17 11452 3:7 12 79:16	123 27:5, 27:6, 46:5, 46:19 128 13:17, 25:19, 29:6, 34:5 14 32:3 143 88:10, 88:12, 89:3, 89:19, 92:14, 94:7 14559 2:9 16 34:4 160 66:12, 68:2, 68:9 17 46:20 2 20 24:4, 66:12, 66:15, 66:18 2003 6:19, 6:22, 7:10 2013 40:13 2023 1:12 2024 1:16, 2:7, 5:2 2029 96:22 206.905 3:20 210 3:18 22 2:7 23001848 2:10 256 13:22, 14:2 26 71:22, 76:10,	76:11 27 72:1, 72:11 28 79:20 3 3 1:17, 2:7, 39:13, 79:11 30 71:22, 72:1, 79:11 300 3:8 31 79:17 33 8:12, 9:6 35 80:2, 83:13, 86:17, 87:2, 87:6 37 19:2, 19:6, 19:11 38 19:2, 31:22 39 34:19, 36:9, 38:16 4 4 39:14 5 5 79:16, 79:17 531921 1:19 54 39:13 56 2:7, 95:2 6 6 2:7, 95:2	6266 1:22, 2:8, 96:20 64 25:20, 29:17, 29:18 678 8:17, 18:17, 19:17, 20:6, 32:5, 37:3, 39:17, 41:5, 41:11, 41:14, 48:4, 48:8, 49:2, 49:14, 49:18, 51:2, 52:8, 55:16, 67:3, 69:1, 69:4, 69:21, 84:13 7 71 44:14, 48:3, 48:19, 55:15, 55:16 8 8-bit 66:13 858.720 3:10 9 9,280,678 1:13 90 17:14 92130 3:9 94 4:9 97 1:20 98101 3:19
--	---	---	--