



Planet Depos®
We Make It *Happen™*

Transcript of Aviel D. Rubin, Ph.D.

Date: November 22, 2024

Case: Datavant, Inc. -v- Vigilytics LLC (PTAB)

Planet Depos

Phone: 888.433.3767 | **Email:** transcripts@planetdepos.com

www.planetdepos.com

Michigan #8598 | Nevada #089F | New Mexico #566

WORLDWIDE COURT REPORTING & LITIGATION TECHNOLOGY

Datavant Exhibit 1014
Datavant v. Vigilytics, IPR2024-00311

1 UNITED STATES PATENT AND TRADEMARK OFFICE

2
3 BEFORE THE PATENT TRIAL AND APPEAL BOARD

4
5 DATAVANT, INC.

6 Petitioner

7 v.

8 VIGILYTICS LLC

9 Patent Owner

10
11 IPR2024-00226

12 Patent No. 9,118,641

13
14 REMOTELY CONDUCTED VIDEOTAPED DEPOSITION OF

15 AVIEL D. RUBIN, PHD

16 FRIDAY, NOVEMBER 22, 2024

17 8:32 A.M. CST

18
19
20 JOB NO.: 562444

21 PAGES: 1 - 147

22 REPORTED BY: KARISA EKENSEAIR, CCR RPR RMR

1 DEPOSITION OF AVIEL D. RUBIN, PHD, CONDUCTED
2 VIA ZOOM VIDEOCONFERENCE.
3
4
5
6
7
8
9

10 Pursuant to notice, before Karisa J.
11 Ekenseair, Certified Shorthand Reporter in and for
12 the States of Arkansas, Oklahoma, Missouri,
13 Illinois, Tennessee, Georgia, New Mexico,
14 Washington, and California; National Registered
15 Professional Reporter; National Registered Merit
16 Reporter; Notary Public in and for the State of
17 Arkansas.
18
19
20
21
22

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

A P P E A R A N C E S

ON BEHALF OF THE PETITIONER (VIA ZOOM) :

JUSTIN OLIVER, ESQUIRE
VENABLE LLP
600 MASSACHUSETTS AVENUE, NW
WASHINGTON, D.C. 20001
202-344-4000

ON BEHALF OF THE PATENT OWNER (VIA ZOOM) :

NICHOLAS STEPHENS, ESQUIRE
JEFFREY BARCLAY, ESQUIRE
FISH & RICHARDSON, PC
RBC PLAZA
60 SOUTH 6TH STREET
SUITE 3200
MINNEAPOLIS, MINNESOTA 55402
612-335-5070

1	T A B L E O F C O N T E N T S	
2		PAGE
3	STYLE AND NUMBER.....	1
4	APPEARANCES.....	3
5		
6	WITNESS: AVIEL D. RUBIN, PHD	
7	EXAMINATION BY MR. OLIVER.....	6
8	EXAMINATION BY MR. STEPHENS.....	139
9	FURTHER EXAMINATION BY MR. OLIVER.....	144
10		
11	CERTIFICATE OF REPORTER.....	146
12		

13	EXHIBITS		
14	(ATTACHED TO TRANSCRIPT)		
15	NUMBER	DESCRIPTION	PAGE
16	EXHIBIT 1001	UNITED STATES PATENT NO.	
17		9,118,641.....	10
18	EXHIBIT 1005	UNITED STATES PATENT NO.	
19		7,823,207, EVENHAIM.....	11
20	EXHIBIT 1006	UNITED STATES PATENT	
21		APPLICATION PUBLICATION NO.	
22		US 2007/0294111, SETTIMI.....	11

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

EXHIBITS		
(ATTACHED TO TRANSCRIPT)		
NUMBER	DESCRIPTION	PAGE
EXHIBIT 1007	UNITED STATES PATENT APPLICATION PUBLICATION NO. 2002/0111833, DICK.....	11
EXHIBIT 1008	UNITED STATES PATENT NO. 7,519,591, LANDI.....	11
EXHIBIT 1009	AMIA 2002 SYMPOSIUM, MURPHY....	12
EXHIBIT 2001	DECLARATION OF AVIEL D. RUBIN IN SUPPORT OF PATENT OWNER'S RESPONSE.....	9

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

2 AVIEL D. RUBIN, PHD

3 of lawful age, being first duly sworn, deposes and
4 says in reply to the questions propounded as
5 follows:

6 EXAMINATION

7 BY MR. OLIVER:

8 Q Good morning, Dr. Rubin. How are you
9 today?

10 A I'm fine, thank you. Good morning.

11 Q I'd like to start with getting a little
12 housekeeping out of the way.

13 Is there any reason you cannot give
14 truthful testimony today?

15 A No.

16 Q You're not taking any medication that
17 would affect your ability to give truthful
18 testimony?

19 A No.

20 Q I'll endeavor to take breaks about every
21 hour or so. Let me know if you need break at some
22 other point. The only thing I ask is that if

1 there's a question pending, you answer the
2 question before we take the break; is that fair?

3 A Sounds good.

4 Q And you understand that your attorney may
5 object during this deposition, but absent an
6 assertion of privilege you will be required to
7 answer all the questions.

8 Do you understand?

9 A Yes.

10 Q I'll try to be clear in all my questions,
11 that's not always the case. If there's any reason
12 you don't understand one of my questions, please
13 let me know and I'll try and clarify.

14 A Okay.

15 Q I'll most often be asking questions
16 relative to the perspective of the person of
17 ordinary skill in the art.

18 Are you familiar with that concept?

19 A Yes.

20 Q For ease of today, I intend to use the
21 acronym P-O-S-A or POSA to refer to the person of
22 ordinary skill in the art.

1 Is that all right with you?

2 A Sure.

3 Q Absent me specifying otherwise, please
4 assume that my question is asking for an answer
5 relative to the POSA's perspective.

6 How did you prepare for this deposition?

7 A To prepare for the deposition I re-read
8 the materials in the case like my declaration, the
9 Clark declarations, the petition, the patents, the
10 prior art references, and then I had a meeting
11 with counsel as well to discuss.

12 Q How many times did you meet with counsel?

13 A One time.

14 Q Do you have any notes with you or in front
15 of you today?

16 A Let me tell you what I have. They're not
17 notes. I have a copy -- so I have a binder
18 here -- well, you can't see it, with a copy of my
19 declaration and the exhibits to that. And on the
20 table I have some of those exhibits. These are
21 just the patents that are the '641 patent and some
22 of the prior art references that I printed out.

1 All of copies of everything are pristine, so I
2 have made no marks, taken no notes on anything.

3 And then on my computer I have just the
4 Zoom window and a PDF viewer that's showing those
5 same documents, some of them that I chose to open,
6 also pristine. And I have the folder that you
7 asked me to download which is I think is a lot of
8 the same documents.

9 Q Are you in communication via text or
10 e-mail with anybody during this deposition?

11 A No.

12 Q Approximately how many times have you been
13 deposed before?

14 A I think around 80.

15 Q And were those depositions instances in
16 which you were serving as an expert witness?

17 A Yes.

18 (Exhibit 2021 marked for identification.)

19 Q Just to get a little administrative work
20 out of the way, you mentioned that you have your
21 declaration in front of you, correct?

22 A Yes.

1 Q And just looking at the cover page, that's
2 for IPR2024-00226?

3 A Yes.

4 Q And it's marked as Exhibit 2021, correct?

5 A Yes.

6 (Exhibit 1001 marked for identification.)

7 Q Do you have Exhibit 1001 in front of you?

8 A What is that?

9 Q That's the '641 patent.

10 A Yes.

11 Q And just for clarity, that is U.S. Patent
12 No. 9,118,641, correct?

13 A Yes.

14 Q Is it okay with you if I refer to that as
15 the '641 patent today?

16 A Yes.

17 Q And do you also have the Evenhaim
18 reference?

19 A Yes.

20 Q And just for clarity, that's been marked
21 as Exhibit 1005, correct?

22 A Yes.

1 (Exhibit 1005 marked for identification.)

2 Q And do you have the Settimi reference?

3 A Yes.

4 Q And just for clarity, that's been marked
5 as Exhibit 1006, correct?

6 A Yes.

7 (Exhibit 1006 marked for identification.)

8 Q And do you have the Dick reference?

9 A Yes.

10 Q And that has been marked as Exhibit 1007,
11 correct?

12 A Yes.

13 (Exhibit 1007 marked for identification.)

14 Q And do you have the Landi reference?

15 A Yes.

16 Q And that has been marked as Exhibit 1008,
17 correct?

18 A Yes.

19 (Exhibit 1008 marked for identification.)

20 Q And do you have the Murphy reference?

21 A Yes.

22 Q And that has been marked already as

1 Exhibit 1009, correct?

2 A Yes.

3 (Exhibit 1009 marked for identification.)

4 Q Great. Let's start with your declaration,
5 if we can.

6 If you could turn to paragraph 5 of your
7 declaration.

8 A Okay.

9 Q And that paragraph extends onto the page 6
10 of your declaration. And in paragraph 5 on
11 page 6, you refer to your latest research focus
12 being on security for healthcare IT systems.

13 Do you see that?

14 A Yes.

15 Q And when you say the "latest research"
16 when did that research start?

17 A I started working on healthcare IT system
18 as a primary focus in 2011.

19 Q And did you do any work in security for
20 healthcare systems prior to 2011?

21 A I did. I worked as a professor Johns
22 Hopkins starting in 2003 and there were projects

1 going on there where I contributed, but I didn't
2 decide to pursue grant funding and make it my
3 primary focus until 2011.

4 Q When were those earlier projects at Johns
5 Hopkins that you just referred to?

6 A I don't remember any of them specifically.
7 I remember going to the medical school and meeting
8 with various doctors who had a lot of knowledge of
9 technology but not a lot of knowledge of security
10 and cryptography and offering them what I would
11 call, you know, consulting-type advice on the
12 projects that they were working on, how to secure
13 various data, how to architect systems.

14 I did a tour sometime in that period of
15 the Hopkins Medical School, different departments
16 like pathology, oncology, the neonatal ICU where
17 there was a doctor who was very interested in
18 medical informatics. And after that, I was
19 starting to gain a lot of interest in how I could
20 apply my field which was security and cryptography
21 to the medical space.

22 Q And about how many projects did you work

1 on at that time prior to let's say 2009?

2 A Your question just said how many projects.

3 I assume you mean that were related to medical

4 because I was -- I was working on other areas,

5 too, at the time.

6 Q Yes. Medical specifically.

7 A At any given time I was involved with

8 maybe two, three, or four projects. I wasn't a

9 PI, like, a principle investigator at the time on

10 medical projects, I was more just interested in

11 them, attending seminars, and providing feedback

12 to the doctors.

13 Q In paragraph 6 of your declaration you

14 refer to your thesis. Can you tell me what was

15 involved in that?

16 A Sure. And are you asking specifically in

17 the technical content of my thesis or what's

18 involved in general in creating a thesis?

19 Q The technical content.

20 A Okay. So my dissertation or thesis was

21 titled, Nonmonotonic Cryptographic Protocols and

22 it had to do with cryptographic protocols where

1 a -- one or more of the parties would discard
2 information as part of the protocol. So previous
3 to this all of the cryptographic protocols in the
4 literature had monotonically increasing
5 information at all of the different parties. And
6 I had a protocol that I had designed for the
7 Kerberos system that involved one of the parties
8 deleting a key and I couldn't find any reasoning
9 systems at the time that would be used to analyze
10 the security of a protocol that would fit it, and
11 so I ended up designing a logic of authentication
12 that could deal with nonmonotonicity and that
13 turned into my dissertation.

14 Q And why would a party delete a key?

15 A So the issue was to have long-running jobs
16 in a hostile environment or post-dated jobs in a
17 hostile environment. So, for example, you might
18 want to have a batch program that you wrote run in
19 three days. And you would stick it on a remote
20 server that perhaps would be attacked in the
21 interim.

22 And so the solution -- summary of the

1 solution is that you would take that -- the job
2 instructions, encrypt them with a key, send the
3 key to a server, and then delete the key on that
4 machine. So if somebody were to break into that
5 machine before the job ran and then let's say you
6 were to recover from that, they wouldn't find the
7 key or be able to see the information in that job.
8 When it's time to run the job, assuming you've
9 recovered from that attack, the server would send
10 the key, the job would be decrypted, and then run.

11 And so the issue was to formulate a
12 mechanism for analyzing the security of that
13 protocol I just described and then I generalized
14 it to all protocols where you might have to delete
15 a key or some other information and then still
16 reason about how secure the system is.

17 Q Can you look at paragraph 18 of your
18 declaration?

19 A Sure.

20 Q In paragraph 18 you refer to an
21 educational program that focused on teaching
22 healthcare IT professionals about the HIPAA

1 privacy and security.

2 Do you see that?

3 A Yes.

4 Q When was that?

5 A So the masters program that I'm referring
6 to was founded in 2002, and I joined in 2003 as
7 technical director. I taught courses in the
8 program and that program is still running today.

9 Q What types of things were taught in that
10 program?

11 A We had a couple of different tracks. So
12 we had the healthcare management track and the --
13 which was more of a policy-oriented track and then
14 we had the technical track. I was the curriculum
15 chair for the technical track. And in the
16 technical track we would teach some of the more
17 core computer security courses with a bit of a
18 focus on healthcare IT as a domain. And then the
19 more policy-oriented courses dealt with -- we had
20 lawyers teaching legal aspects, we had a couple of
21 courses in the business school about managing
22 security in a -- large health organizations,

1 things like that.

2 Q For the technical track, would that track
3 have taught things like tokenization for instance?

4 A At some point in the curriculum, and I
5 can't recall when, there would have been coverage
6 of that topic.

7 Q What about normalizing data in databases,
8 would that have been something that would have
9 been covered in that track?

10 A What do you mean by normalizing data?

11 Q How do you understand the term
12 "normalizing" to be used in the field of
13 databases?

14 A I think it would be application specific.
15 For example, if you had -- let's say you were
16 talking about preventing the fingerprinting of a
17 network by looking at the timing of packet
18 arrivals. So normalizing might mean rounding the
19 timings down before putting them in the database
20 and that was a technique that we did teach with
21 respect to fingerprint of network analysis.

22 Q What about the term "normalizing" in the

1 context of ensuring that information such as a
2 person's name or other identifying information is
3 recorded in a consistent way across different
4 entities?

5 MR. STEPHENS: Objection, form.

6 A I see. So I am familiar with that problem
7 and that issue. I did not cover that in the
8 courses that I taught, so I don't know if that was
9 covered in any of the courses.

10 Q You said you're familiar with that concept
11 or I guess more specifically you said you're
12 familiar with that problem.

13 Can you explain what you mean by "that
14 problem"?

15 A So one project that I've worked on had to
16 do with merging databases from different
17 organizations. For example, let's say that two
18 healthcare companies are merged or one acquires
19 the other and they have medical record databases.
20 If the same patient went to both of those
21 facilities, they would want to ensure that they
22 didn't end up with a system that had two different

1 representations for the same patient, they would
2 want all of those records to be merged. And
3 that -- that's -- that problem arises in many
4 domains, not just in medical, but it definitely
5 arises in medical.

6 Q And when was that project that you just
7 referenced?

8 A I don't remember.

9 Q What other domains does that problem arise
10 in?

11 A So, for example, if you have school
12 districts where students transfer from school to
13 school, and maybe the two districts would combine
14 their IT systems.

15 Another one would be voter registration
16 when your -- you want to maybe detect if
17 somebody's tried to register to vote in more than
18 one location, things like that.

19 Q When did you first become aware of that
20 issue in your database work?

21 A I don't remember.

22 Q Can you turn to paragraph 58 of your

1 declaration.

2 A 58?

3 Q Yes.

4 A Okay. I'm there.

5 Q And 58 includes a footnote, Footnote 1.

6 Do you see that on page 22?

7 A Yes.

8 Q Can you explain what you meant by Footnote
9 1.

10 A Yes. So Footnote 1 is basically saying
11 that if you have the identified healthcare
12 information it should not be released to someone
13 who has the -- the personally identifiable
14 information like the names, for example, that were
15 used to generate that request because if you do
16 that it would be possible to perhaps match those
17 names with the -- the de-identified records thus
18 reversing the de-identification and identifying
19 them.

20 Q If someone makes a request for a specific
21 patient records and there's a system for providing
22 that, doesn't the requester know what names were

1 requested to begin with?

2 MR. STEPHENS: Objection, form.

3 A So in this footnote I'm talking about when
4 records are released to a third party, so that
5 wouldn't be the requester; that would be somebody
6 else.

7 Q What might be an example of the third
8 party you're referring to?

9 A It could be a research database, for
10 example.

11 Q Could it be some sort of clearinghouse for
12 requests for data?

13 A So your question is whether a request for
14 de-identified medical information could go to a
15 clearinghouse?

16 Q Yes.

17 A It could in a system that you could build.

18 Q Staying in paragraph 58 of your
19 declaration, at the very end there is a figure,
20 Figure 3 from the '641 patent.

21 Do you see that?

22 A Yes.

1 Q Did the problem you describe in Footnote 1
2 happen in Figure 3?

3 A No.

4 Q And why not?

5 A Because the -- the encryption server does
6 not see the medical information, the user does not
7 see the medical information in a form where it can
8 be matched to the names, it just gets a report
9 which in this patent is -- is -- contains some
10 kind of a score, and so there's no place where the
11 third party gets access to the PII that was used
12 to generate the request and to the medical
13 information.

14 Q And when you say the third party, you're
15 talking about the encryption server?

16 A Well, neither the encryption server or the
17 user, but, yes, in this instance the encryption
18 server does not get that information.

19 Q And what's the purpose of the encryption
20 server 312 in Figure 3, and specifically is it
21 acting as some sort of escrow agent?

22 A So the purpose of the encryption server is

1 to produce tokens from a request based on the
2 individuals in the request.

3 Q So it has the key or other mechanism for
4 changing identifying information into a token,
5 correct?

6 A Well, there doesn't necessarily have to
7 even be a key because it could use an unkeyed
8 hashed function to do it.

9 Q But otherwise, it does include whatever
10 mechanism would be used to create that token?

11 A What was the word, it does what?

12 Q It includes whatever mechanism would be
13 used to encrypt or create that token?

14 A Yes. It creates the token so it has to
15 have the mechanism.

16 Q Would that be an example of an escrow
17 agent in sort of the field of cryptography?

18 A I wouldn't consider it that.

19 Q What would you consider an escrow agent to
20 be?

21 A An escrow agent -- let me give you an
22 example of how it's traditionally used.

1 In the early 90s or mid 90s, the U.S.
2 government did not want to allow communications to
3 be encrypted unless the keys were stored somewhere
4 that the government could get to them, so they
5 devised a system where there was a server that
6 would have keys that could be used to bypass the
7 security of any communications and those keys
8 would be held in that server and so they would be
9 escrowed there.

10 Q So in that instance the server was holding
11 encryption keys?

12 A Yes.

13 Q In Figure 3, what's the relationship of
14 the controlling entity or entities for encryption
15 server 312 and the data server 318?

16 A I'm going to pull up the patent. You're
17 asking 312 and --

18 Q 318.

19 A 318, okay. So the patent describes more
20 about the functionality of -- of what they send to
21 each other and how they communicate than what the
22 relationship is between them.

1 Q What would a POSA understand to be the
2 relationship between server 312 and server 318
3 with respect to, for instance, who controls them?

4 A The thing a POSA would understand is that
5 the encryption server 312 and the server at 318 do
6 not really share all of their information. So any
7 relationship where they keep their information
8 separate would work.

9 Q Would they be under the control of the
10 same company, for instance?

11 A I don't think it would matter as long as
12 they had a process of making sure that they didn't
13 share information.

14 Q Could they be controlled by different
15 companies?

16 A They could be.

17 Q If they were controlled by different
18 companies, would a POSA expect that there would be
19 some sort of agreement between those two
20 companies?

21 A Well, at the very least there would have
22 to be coordination of what the message passing

1 would look like between them. For example, the
2 encryption receiver couldn't send request tokens
3 to a server that wasn't expecting to receive them.

4 Q Again, looking at Figure 3, what would
5 prevent someone at encryption server 312 from
6 initiating the request message as the user?

7 A So you're saying would the encryption
8 server be able to impersonate a user?

9 Q Yes.

10 A I don't believe that that scenario is
11 addressed in the patent.

12 Q Yeah. I'm just asking if a person of
13 ordinary skill in the art would understand that's
14 possible.

15 A I'm not sure. I haven't considered it.

16 Q Do you know how a person of ordinary skill
17 in the art would guard against that scenario?

18 MR. STEPHENS: Objection, form; scope.

19 A That's -- that's also something that
20 I -- that I haven't considered.

21 Q What prevents the encryption server 312
22 from sharing the token generator with the user or

1 the public?

2 A Well, in the invention, the encryption
3 server doesn't do that and I don't know about
4 another hypothetical system in which one could do
5 that.

6 Q When you say doesn't do it, what prevents
7 it from doing that?

8 A There's no description in the patent of
9 the encryption server doing that, so that's not
10 something that the patent suggests as part of the
11 invention.

12 Q Does the patent describe how it would
13 prevent that from happening?

14 A A POSA would understand that it would
15 apply known security techniques to prevent
16 information that should be only on the encryption
17 server from leaking out.

18 Q And what would those techniques be?

19 A Well, it would depend on the hardware and
20 software architectures on the, you know, things
21 like firewalls, proper authentication, virus
22 checking, things like that.

1 Q Those are technical solutions.

2 What about if whomever is controlling the
3 encryption server just decides to do it or not to
4 put in place those preventions? What prevents
5 that person from disseminating the token
6 generator?

7 A So you're saying if there's a person there
8 who is -- so -- so are you in a hypothetical
9 system that's different from ones described in the
10 patent?

11 Q Well, you've told me the patent doesn't
12 describe how this takes place.

13 So I'm asking sort of how a person of
14 ordinary skill in the art reading the patent would
15 understand, if any, ways to prevent whatever
16 entity that controls the encryption server from
17 disseminating the token generator?

18 A I think one of skill in the art would
19 consider the technical means that would be needed
20 that I described.

21 Q And, again, I'm saying beside the
22 technical means, if there's an entity that

1 controls that, they also control the technical
2 means.

3 So what prevents that entity from
4 disseminating the token generator if that entity
5 chooses to do so?

6 A So I think in that hypothetical scenario
7 it would be either a contractual agreement or just
8 an understanding that the point of this encryption
9 server is that it should not be sharing all of its
10 information with the public.

11 Q Can you turn to the '641 patent?

12 A Sure.

13 Q And specifically, claim 7 on the last page
14 of the patent.

15 A Okay.

16 Q So in the context of the problem you
17 described in Footnote 1 of your declaration in
18 paragraph 58 of your declaration, I'd like to talk
19 if there's any mechanism in the context of claim 7
20 that prevents a third party from having access to
21 both the personal identifying information and the
22 token generation mechanism. And I'll explain that

1 in more detail if it would be helpful.

2 A Sure.

3 Q Looking at claim 7 in column 11 at line --
4 around 12, there's a reference to a request for
5 healthcare information, correct?

6 A Yes.

7 Q But claim 7 doesn't limit from whom that
8 request derives, correct?

9 A I -- I haven't considered that question
10 before, but -- but looking at it, I don't see a
11 limitation there.

12 Q So claim 7 doesn't seem to preclude the
13 requester and the encryption server from being the
14 same thing, correct?

15 A I -- I think it does because claim 7 is in
16 the context of this patent and this patent
17 describes a system which is illustrated, for
18 example, one embodiment in claim 3 -- in Figure 3
19 where it shows the encryption server and the
20 requester as being separate and that is consistent
21 with the description in the specification.

22 Q So it seems, though, you are reading into

1 claim 7 the design in Figure 3, correct?

2 MR. STEPHENS: Objection, form.

3 A I -- I wouldn't say that's what I'm doing.
4 What I'm doing is saying that this patent
5 describes a certain architecture and describes a
6 certain functionality and that the claim is read
7 in the context of the specification.

8 Q But is there any specific preclusion from
9 the encryption server being the same as the
10 requester?

11 A I'm pulling up my declaration to see if I
12 discuss that. I don't see that I discuss that
13 question anywhere in my declaration, so if I do
14 you can point me to it, but otherwise, I don't
15 have an opinion on that.

16 Q Looking again at claim 7 in column 11
17 starting at line 31.

18 A Okay.

19 Q There the claim states: Providing the
20 produced healthcare information.

21 Do you see that?

22 A Yes.

1 Q Is it correct that that step does not
2 identify to whom or to what the healthcare
3 information is reported?

4 A So those words do not appear in claim 7.
5 There is, for example, in one embodiment described
6 in Figure 3, it shows that the report is sent back
7 to the user and I have not performed the analysis
8 yet as to whether that embodiment is limiting on
9 the claim. So that -- that might be something I
10 would work on later in the case or if it's in my
11 declaration I would be happy to address it.

12 Q Would a person of ordinary skill in the
13 art implement claim 7 in a way that complied with
14 HIPAA?

15 A I would say that they -- they typically
16 would.

17 Q And why is that?

18 A Because this is a -- one of the
19 motivations for architecting the solution the way
20 that it is, is to keep one party from being able
21 to break the de-identification of the data which
22 is consistent with the HIPAA requirements, and one

1 working in this field at the time of the invention
2 would have known that for a system to be useful
3 and deployed in the United States it would need to
4 be compliant with HIPAA.

5 Q Can you turn to paragraph 60 of your
6 declaration, please?

7 A Okay.

8 Q And the first sentence refers to
9 identities of individuals being unattainable from
10 tokens.

11 Do you see that?

12 A Yes.

13 Q And what does it mean to be unattainable
14 from the tokens?

15 A I'm not sure what part of that isn't
16 clear.

17 Q Well, let me give an example.

18 If the token was created with an
19 encryption mechanism and someone holds the key to
20 decrypt it, would that still be considered
21 unattainable?

22 A No.

1 Q So whenever there's a key for decryption,
2 it wouldn't qualify as token creation in the
3 context of the '641 patent?

4 A I would say that if the -- if the
5 tokenization can be reversed, then it wouldn't be
6 HIPAA compliant.

7 Q So if anyone held a key that could
8 reidentify in your opinion, it wouldn't qualify as
9 tokenization in the '641 patent?

10 MR. STEPHENS: Objection, form; scope.

11 A That's not what I said.

12 Q Well, then maybe explain it because that
13 sounds like what you were saying.

14 A No. I said HIPAA has a -- the HIPAA rule
15 states that if you can reverse the tokens, then
16 you're not in compliance.

17 Q So your understanding is that under HIPAA,
18 if a key exists for reversing the encryption of a
19 token, that would not qualify under HIPAA?

20 A I would need more specifics about the
21 example and I would have to pull up the HIPAA
22 rule. But there are requirements in HIPAA about

1 the irreversibility of tokens.

2 Q What if the covered entity under HIPAA had
3 the key for reversing the encryption?

4 A I would need to look into that.

5 Q What if the business associate of a
6 covered entity had the key for reversing the
7 encryption?

8 A I -- I think -- you know, HIPAA compliance
9 is -- is something that takes weeks of work and
10 analysis. I can't just sit here and -- and make
11 judgments about whether a hypothetical with little
12 information is HIPAA compliant.

13 Q In that same paragraph of your
14 declaration, paragraph 60, you refer to the tokens
15 are reproducibly irreversible.

16 What's meant by that term?

17 A I have a citation to look at and so I'm
18 going to take a look at that. It means that the
19 process -- the tokens cannot be reversed, but if
20 you were to generate the tokens again the same
21 way, you would get the same token if you started
22 with the same data.

1 Q And can symmetrical encryption be used for
2 HIPAA-compliant tokenization?

3 A I don't address that in my report. I
4 would need to do some research on that.

5 Q So sitting here today you're not sure of
6 the answer to that question?

7 A Yes.

8 Q In paragraph 60 of your declaration on the
9 last line of that paragraph you refer to a hash
10 function.

11 Do you see that?

12 A Yes.

13 Q Can you explain what a hash function is?

14 A Sure. Hash function is a well-known
15 primitive in cryptography and what it does is it
16 takes what's called a pre- image which is an input
17 and then it produces an output which is a fixed
18 length and -- which has the property that it's
19 infusible to define two different pre-images that
20 hash to the same value. It also has the property
21 that you can't start with the output and find a
22 pre-image.

1 Q And what do you mean by pre-image?

2 A That's the input. So let's say I want
3 to -- I have a file and I want to hash its
4 contents, the contents of the file are the
5 pre-image.

6 Q So a hash function is a manner of
7 encrypting that can be used to create a token?

8 A Within the context of the '641 patent,
9 that is correct.

10 Q What's a one-way hash?

11 A The hash function that I described is one
12 way. It's the fact that you cannot find a
13 pre-image given a hash function output.

14 Q Look at paragraph 61 of your declaration.

15 A Okay.

16 Q And you refer to a data aggregator in the
17 second line of that paragraph.

18 Do you see that?

19 A Yes.

20 Q And what do you mean by data aggregator?

21 A So the data aggregator that I'm referring
22 to here is the de-identified data server which

1 would be the middle server in the box in Figure 3.

2 Q And that middle server 318 has a database
3 320, correct?

4 A Yes.

5 Q And that database has only de-identified
6 data and tokens, correct?

7 A That's all that's shown in the figure
8 here.

9 Q So that would be sort of a centralized
10 warehouse of data that came from the various
11 source sites 138, correct?

12 A Yes.

13 Q And what does it mean to be an aggregator?

14 A It means you collect information from
15 different places and you store it all together.

16 Q And in this case, the different places
17 would be the various source sites?

18 A Yes.

19 MR. OLIVER: We've been going for about an
20 hour. Why don't we take a five-minute break.

21 (Whereupon a break was had.)

22 BY MR. OLIVER:

1 Q Dr. Rubin, can you turn to paragraph 74 of
2 your declaration?

3 A Okay.

4 Q And in paragraph 74, there's a list of
5 terms and their corresponding constructions.

6 Do you see that?

7 A Yes.

8 Q And for the term "token," the construction
9 stated is: An identifier associated with an
10 individual that does not reveal the identity of
11 the individual.

12 Do you see that?

13 A Yes.

14 Q Do you agree with that construction?

15 A I agree. I applied that construction in
16 my analysis and I agree with it. I -- I haven't
17 actually analyzed whether it's correct or not, I
18 just adopted it.

19 Q So under that understanding, a token could
20 be some sort of ID that is used in place of
21 identifying information for an individual?

22 A That seems to follow.

1 Q Would encrypting a person's name be a type
2 of tokenization?

3 A Well, it depends.

4 Q And what would it depend on?

5 A On whether the encryption key was
6 available, because the construction says that it
7 does not reveal the identity of the individual.
8 So if I encrypt a person's name and then release
9 the encrypted name with the key, then it would
10 reveal it.

11 Q So the key would have to be kept
12 confidential?

13 A It would have to be never accessible or
14 destroyed.

15 Q Before 2009, did you have experience with
16 tokenization?

17 A I don't recall.

18 Q You don't recall if you had experience
19 with tokenization before 2009?

20 A Right.

21 Q Did you have experience with token
22 matching before 2009?

1 A If you're referring to matching tokens in
2 a medical database, then I don't recall if I
3 worked on anything like that before 2009.

4 Q What about outside of the medical field?

5 A I don't recall if I specifically worked on
6 anything like that.

7 Q Before 2009, what experience did you have
8 with de-identification?

9 A I don't recall if I had any.

10 Q In the field of cryptography are you
11 familiar with a plain text attack?

12 A I believe you're referring to known plain
13 text.

14 Q I believe there are two, are there not,
15 chosen and known?

16 A Well, yeah. So it's -- you said a plain
17 text attack, so I guess my answer to that question
18 is no.

19 Q Your answer to what question?

20 A Am I familiar with an attack known as a
21 plain text attack. It's either got to be known
22 plain text or chosen plain text or something plain

1 text; it's not just a plain text attack.

2 Q Well, then are you familiar with a chosen
3 plain text attack?

4 A Yes.

5 Q And can you explain what that is?

6 A It's where the attacker has the
7 ability -- it's basically a model of an attacker
8 in the chosen plain text attack model. You assume
9 that the adversary has the ability to pick any
10 plain text and receive an encryption of it.

11 Q And what's a known plain text attack?

12 A That's where an adversary would have
13 access to plain text cypher text pairs, not
14 necessarily of their choosing, but just ones that
15 they are able to get their hands on.

16 Q And what are some of the -- well, let me
17 back up.

18 When did you first become aware of these
19 different types of plain text attacks?

20 A Probably 1991.

21 Q And what are some of the ways that those
22 in the field guarded against chosen and known

1 plain text attacks?

2 A Bigger keys.

3 Q And how did bigger keys guard against
4 those types of attacks?

5 A Because the attacks that you can launch
6 with known plain text or chosen plain text are
7 attacks that attempt to minimize or reduce the key
8 space that's needed for exhaustive search. And so
9 if you have a large enough key search, then even
10 with those attacks -- like with today's cyphers
11 with 128-bit keys, for example, AES, you are
12 resistant to chosen plain text attacks. But if
13 you were to zero out all but say 45 bits of the
14 key, then chosen plain text attack would work and
15 would a be -- would make it a lot easier than an
16 exhaustive search attack.

17 Q In your answer you referenced AES. Can
18 you describe what that is?

19 A AES stands for Advance Encryption
20 Standard. That is a NIST standard that has been
21 adopted widely by the banking industry and by many
22 other industries as well.

1 Q And for the ease of the life of the court
2 reporter, you said NIST. Can you state that
3 acronym for the record?

4 A Sure. It's the National Institute of
5 Standards and Technology.

6 Q Are you aware of an option called --
7 excuse me, salt being used to guard against
8 different types of plain text attacks?

9 A Yes.

10 Q And what is that?

11 A So to salt a plain text, what you do is
12 you append a random value to the beginning of it
13 and that way -- let's say that you were to pick a
14 random salt every time you perform an encryption,
15 then you encrypt the same value with a -- with an
16 encryption function that has a random salt. You
17 would get a different output. And then when you
18 decrypt you can just subtract the salt back out.
19 And so it's a way of mismatching plain texts and
20 cypher texts.

21 Q And when were you first aware of the use
22 of salt?

1 A Probably same time, 1991.

2 Q Are you aware of cypher block chaining as
3 a way to prevent against different types of plain
4 text attacks?

5 A Yes.

6 Q And can you explain what that is.

7 A So in cypher block chaining you would take
8 the output of an encryption block and
9 exclusively -- or with the input of the next
10 encryption block and thus you're chaining all of
11 the blocks together, and that is used to -- it's
12 actually not so much used to prevent different
13 types of plain text attacks, but something called
14 a cut-and-paste attack where an attacker takes a
15 portion of an encrypted message out and puts it
16 into another message.

17 The classic example of that is let's say
18 that I had a file that contained all of the
19 employee HR information and it was encrypted with
20 AES and you didn't do any block chaining. So I
21 could take your boss' encrypted file and -- and
22 cut out the piece that contains the salary and

1 paste that into my HR file in the salary field and
2 it would decrypt correctly because it was
3 encrypted with the proper key.

4 But if you cypher block chain, you can't
5 do that because all of the bits that are in the
6 message affect the encryption, so you can't
7 decrypt it without all of the bits being proper.
8 So it provides an integrity safeguard.

9 Q And when did you first become aware of
10 cypher block chain?

11 A 1991 time frame.

12 Q In the context of searching healthcare
13 records, would there be a difference between the
14 type of search that was performed by, for
15 instance, an insurance company looking to
16 determine insurance risk for a group of patients
17 and a search by a pharmaceutical company looking
18 for patients for a clinical study?

19 A Can I hear that again, please?

20 Q Let me break it apart to make it a little
21 more digestible.

22 A company like an insurance company might

1 want to search for the health records of specific
2 patients so as to determine the risk of insuring
3 that population, correct?

4 A Yes.

5 Q And in that case the insurance company's
6 type of search would be one for specific patients,
7 correct?

8 A Well, not necessarily. They -- if we look
9 at the '641 patent, for example, it provides a
10 means for getting a risk score for a whole group.

11 Q That group would then have specific
12 patients, correct?

13 A Yes.

14 Q So the insurance company would be looking
15 for the health records for a group of particular
16 patients?

17 A Well, again, in what I -- what I'm trying
18 to draw the distinction here in the '641 they're
19 not going to get that, they're going to get a
20 group score. They're going to input a bunch of
21 specific patients, but the thing that they're
22 searching for and that they're going to get is

1 going to be the group score.

2 Q So the query would be for particular
3 patients?

4 A It would include the patients, yes.

5 Q Or a pharmaceutical company looking for
6 patients that might be well positioned for a
7 clinical study, the query might be different,
8 correct?

9 A Right.

10 Q And that's because the pharmaceutical
11 company doesn't know the individuals; it knows,
12 for instance, the conditions that are to be
13 studied, correct?

14 A It depends on the scenario, but for
15 clinical trial they're trying usually I would
16 imagine to get the individuals as the output and
17 the input might be some condition or some
18 information that quantifies which people would be
19 good for the study.

20 Q In each type of query that we just
21 discussed the relevant information would come from
22 the pool of patient healthcare records at issue,

1 correct?

2 A Are you specifically referring to the
3 results of the query?

4 Q I am referring to the pool of data that
5 would be searched.

6 A I see. So -- so in general with this
7 example you're giving, you would -- you would look
8 through medical data repository.

9 Q For either of those types of searches?

10 A I would assume so.

11 Q And it might be the same repository of
12 data?

13 A If -- if enough information to satisfy
14 both of those types of queries is in that
15 database, then it could be the same database.

16 Q Can you turn to the Evenhaim reference,
17 Exhibit 1005?

18 A Okay. I've got it on the screen.

19 Q And if you could turn to column 8, please
20 starting at line 39.

21 A Okay.

22 Q 39 states that: The parameter list would

1 include a definition of the population to be
2 analyzed such as by geography, age, or other
3 attributes. One of the most novel features of the
4 instant protocol is that the parameter list may
5 even include specific individuals by name or ID or
6 the like.

7 Correct?

8 A That's what it says.

9 Q So this is indicating that the query might
10 include specific patient names, correct?

11 A I just want to read surrounding text for
12 context.

13 So the question is whether the query could
14 include information about specific individuals?

15 Q Correct.

16 A Yes.

17 Q Can you turn to column 12 of Evenhaim
18 starting at line 63?

19 A Okay.

20 Q And there's a reference there to a key
21 that may be held by an escrow agent.

22 Do you see that?

1 A Right.

2 Q And in this context, what's your
3 understanding of an escrow agent?

4 A I think it's -- it's the same escrow agent
5 we were talking about before that can hold keys
6 for part of a protocol.

7 Q Could the escrow hold keys for encryption
8 and decryption or both? And I'm speaking
9 generally.

10 A Oh, there's nothing about escrow agents
11 that prevents them from holding different types of
12 keys in general.

13 Q And looking back at that same section it
14 says: A trusted third party such as an escrow
15 agent.

16 Do you see that?

17 A Yes.

18 Q What's your understanding of a trusted
19 third party?

20 A It's a party that's not one of the
21 participants in the protocol itself. It's trusted
22 by the participants to behave properly and

1 competently.

2 Q And that would include maintaining
3 confidential information perhaps?

4 A That is one way you could use a trusted
5 third party.

6 Q Are trusted third parties used in medical
7 databases?

8 A So the literal understanding of that
9 question is confusing to me. It's -- you know,
10 the -- are the trusted third parties in the
11 database, meaning are they a record in the
12 database or something like that? So maybe you
13 can --

14 Q In the field of medical data records and
15 the privacy of the same, are trusted third parties
16 used?

17 A They can be.

18 Q Can you turn to column 12, line 36 of
19 Evenhaim?

20 A Okay.

21 Q And in that paragraph there's references
22 to a one-way hash and AES.

1 Do you see that?

2 A Yes.

3 Q And that would be the same one-way hash we
4 discussed earlier, correct?

5 A Yes.

6 Q And AES is the encryption standard that
7 you brought up earlier in our discussion, correct?

8 A Yes.

9 Q And can both of those be used to create
10 tokens?

11 A A one-way hash function can be. With
12 respect to AES, it would depend.

13 Q And what would it depend on?

14 A On how the key is handled after the
15 encryption is applied to the information.

16 Q And what would be some examples of how the
17 key would be handled to protect the tokenization
18 process?

19 A Well, if the key were just discarded, then
20 I would say that that -- that would be a token.

21 Q Can you turn to Evenhaim at column 13?

22 A Okay.

1 Q And in that first paragraph on column 13
2 in the last sentence around lines 19 and 20, it
3 states that: The identity of the person is not
4 knowable to that analyzer.

5 Do you see that?

6 A I see that.

7 Q And what would your understanding be or
8 what would POSA's understanding, rather, be of not
9 knowable to the analyzer?

10 A I need to read the paragraph. It means
11 that the -- someone analyzing whether or not it's
12 the same person wouldn't -- could do that without
13 knowing which person it is.

14 Q You said could do that.

15 What do you mean by could do that?

16 A The compare -- the analysis as to whether
17 the -- it's the same person at the two pharmacies,
18 for example.

19 Q Got it. And who would be the analyzer in
20 this situation?

21 A It -- the patent says one could analyze,
22 so anyone who wanted to perform that analysis I

1 suppose.

2 Q So, for instance, the aggregator that's
3 taking the information from different pharmacies
4 could perform that analysis?

5 MR. STEPHENS: Objection, form.

6 A I think what the -- just the English
7 language understanding of this is "one could
8 analyze" means that if one has the information
9 needed to perform this analysis like the records
10 from the two pharmacies, then one could analyze
11 whether that person is compliant and persistent in
12 refilling the prescription for his medication.

13 Q Earlier in that same paragraph in column
14 13 starting around line four, there's a discussion
15 of encryption that uses more than a single ID.

16 Do you see that?

17 A Yes.

18 Q And there's reference there to the use of
19 two keys.

20 Do you see that?

21 A Yes.

22 Q And what would be the purpose of using two

1 keys in that fashion?

2 A Different data, the different data
3 sources.

4 Q And why would two keys be helpful in that
5 situation?

6 A The -- Evenhaim states that: Because of
7 the fact that we encrypt several key that can
8 uniquely -- I think it should say keys, that can
9 uniquely identify the person, we can link their
10 healthcare record for a more complete analysis.

11 Q So there might be multiple keys relating
12 to the same individual?

13 A I think that's what's being described
14 here.

15 Q Can you turn to column 8 of Evenhaim
16 starting at line 49.

17 A Okay.

18 Q And between lines 49 and 53, there's
19 reference to a query being sent as well as that
20 query being in a format that is mutual -- probably
21 should say mutually agreed to by the aggregator
22 and each respective source entity.

1 Do you see that?

2 A Yes.

3 Q In the context of database searching,
4 what's the importance of a mutually agreed upon
5 format?

6 A It's a compatibility issue.

7 Q And is the idea that if one data source
8 uses one type of terminology and another data
9 source uses of another type of terminology the
10 searching of the records might become complicated?

11 A That would be part of it.

12 Q What would be another part?

13 A The records might not fit. Like, you
14 might have a field that's not long enough to fit a
15 value.

16 Q So the goal in taking the information from
17 the various data sources would be such that the
18 information can be put together in a searchable
19 database in a format that's going to allow robust
20 searching?

21 A So there are reasons other than trying to
22 search the data together in Evenhaim for having a

1 mutually agreed upon format. In fact, it's not
2 really related to the searching because in
3 Evenhaim, the searching happens at the source of
4 the data. And then in order to have compatibility
5 with information coming from different sources,
6 there has to be an agreement on the format.

7 Q And what do you mean by format?

8 A Like, for example, everything from NDNS,
9 whether you store the high-level bits to the left
10 of memory or to the right of memory, to the sizes
11 of different fields, to the names of different
12 fields. If you don't mutually agree upon the
13 format, then you can't really communicate.

14 Q Can you look at column 10 of Evenhaim
15 starting around line 37?

16 A Okay.

17 Q And there's a discussion there of
18 crunching together data items and there's an
19 example given of similar names with variations
20 such as a nickname, a prefix, a suffix, etcetera.

21 Do you see that?

22 A Yes.

1 Q What's being discussed there?

2 A So that's discussed a little more in
3 column 9, line 47. It says: Crunching together
4 may involve name matching through fuzzy logic and
5 other name-mapping algorithms of the population
6 defined by the parameter list with the source
7 entry database names.

8 The basic idea is if you have Nick and
9 Nicholas and it's the same person, you don't want
10 to have separate records for them, you could
11 consider that one.

12 Q And what are the different ways to achieve
13 that?

14 A What it says here is: Joining data items
15 having a mutual or similar microdata specific
16 structure. So using joins.

17 Q Would a person of ordinary skill
18 understand there are other ways to achieve that
19 goal?

20 A There probably are. I haven't considered
21 that.

22 Q What about normalizations, is that used in

1 connection with ensuring consistent formats and
2 terminologies?

3 A I believe that's the goal of
4 normalization.

5 Q How would a POSA understand that one would
6 achieve normalization in forming tokens so that
7 similar records could be identified longitudinally
8 across a system?

9 A I -- I haven't considered that in
10 preparing for this deposition. That's not
11 something in my report.

12 Q Do you know how a POSA would go about
13 doing that, though?

14 A I could probably sit down and come up with
15 ways of doing it, but I -- but I haven't given
16 that any thought before.

17 Q Can you turn to Evenhaim column 10
18 starting at line 29?

19 A Okay.

20 Q And in that paragraph there's a reference
21 to identity-free microdata.

22 A Yes.

1 Q And what would be POSA's understanding of
2 identity-free microdata?

3 A A piece of data that does not contain the
4 identity of a person.

5 Q And what does it mean to be microdata?

6 A Just referring to the fact that you're
7 looking at a -- a small piece, like, maybe a field
8 in a record or something like that. You're not
9 looking at a large database entry.

10 Q Can you look at column 12 of Evenhaim
11 starting at line 48? And in that paragraph
12 there's a reference to micro-level records.

13 Do you see that?

14 A Yes.

15 Q In the context of healthcare records, what
16 would a person of ordinary skill in the art
17 understand to be micro-level records?

18 A It could be one small data that isn't
19 necessarily at the level of a full database
20 record. So, for example, let's say you have a
21 record with someone with a particular disease
22 that's a particular height and you have all -- you

1 know, 20 things in the database and you just look
2 at the disease that they have. So that would be a
3 micro-level record.

4 Q So the micro level might be the specifics
5 of the healthcare conditions of one particular
6 patient?

7 A That would be one example.

8 Q And in that same paragraph the reference
9 to the ability to link micro-level records, is
10 that referring to the ability to link different
11 records for the same patient together?

12 A I'm just going to read some surrounding
13 text for context.

14 Can I -- I don't remember what you asked
15 now.

16 Q Sure. The reference to the ability to
17 link micro-level records, is that referring to the
18 ability to link different records for the same
19 patient together?

20 A Yes.

21 Q Can you turn to Evenhaim at column 3
22 starting around line 32?

1 A Okay.

2 Q In that paragraph on the first line
3 there's a reference to physician-level data.

4 Do you see that?

5 A Yes.

6 Q What's physician-level data?

7 A So it's the data in the form that it is
8 when it's given to the physician.

9 Q When it's given to the physician?

10 A So pharmacy datasets are typically
11 aggregated to the physician or prescriber level,
12 so when they're -- when the data is aggregated in
13 such a way that it is now at the physician level.
14 So that's the level of the physician.

15 Q But does that mean that it's aggregated in
16 a way that the data indicates, for instance, the
17 number of prescriptions for a particular drug that
18 that physician issued without identifying the
19 details as to whom those prescriptions were
20 issued?

21 A That is the example described in this
22 paragraph.

1 Q So the aggregation of physician-level data
2 would be sort of a pool of healthcare information
3 related to the group of patients that the
4 physician treats, but perhaps not in any way that
5 would allow the identification of specific patient
6 records; is that fair?

7 A That's the premise it's starting from. So
8 it says: Aggregated de-identified data physician
9 level. So it's talking about in this example here
10 data that's been aggregated and de-identified so
11 that you cannot tell an individual anything about
12 a particular individual, but you can look at the
13 total number of prescriptions.

14 Q And that total number of prescriptions is
15 as prescribed by that particular doctor?

16 A I think that would be a piece of
17 information that you would expect to see at the
18 physician level.

19 Q And the term "lower resolution" is used in
20 that paragraph.

21 What's meant by lower resolution?

22 A It means that some of the original data

1 set has been lost and is not available for
2 analysis.

3 Q Can you turn to Evenhaim at column 16
4 starting at line 63?

5 A Okay.

6 Q And there Evenhaim states that: One
7 cannot query or analyze parameters that are no
8 longer in the lower resolution data set; therefore
9 the existing healthcare analytics model does not
10 provide the capability to aggregate the behavior
11 of a group of patients by a predefined list of
12 consumers participating in a health program.

13 Do you see that?

14 A Yes.

15 Q What's meant by that?

16 A I need to read the paragraph.

17 So this is discussing a limitation in
18 performing analysis on low-resolution data and
19 it's saying that the existing healthcare analytic
20 model does not provide the capability to combine
21 the behavior of a group of patients from a
22 predefined list because there may not be enough

1 data that's needed to perform the analysis.

2 Q And that same paragraph talks about high
3 resolution data, correct?

4 A Could you show me where?

5 Q Sure. Column 16 appearing at line 49.

6 A Well, here it's just saying that through
7 the aggregation process, high-resolution raw data
8 is reduced to lower resolution data for privacy
9 reasons.

10 Q And that was in what Evenhaim describes as
11 existing services, correct?

12 A Right.

13 Q And the goal that Evenhaim was trying to
14 achieve is to be able to search through records
15 that have micro-level data, correct?

16 A So Evenhaim wanted to be able to search
17 through high resolution data that would have that
18 micro-level data which is why his system involves
19 performing the searches at the source site.

20 Q Would a POSA have understood that one
21 could aggregate data and maintain high-resolution
22 information?

1 A Not if they wanted to be compliant with
2 the privacy standards.

3 Q And what do you mean by that?

4 A For example, HIPAA lists 18 different
5 fields that should be taken out to preserve
6 privacy like birthday, ZIP code, you know, name,
7 etcetera, social security number. So if -- let's
8 say that a researcher wanted to study the spread
9 of COVID in a particular area. If the data had
10 been de-identified and people's ZIP codes had been
11 taken out, then they wouldn't have the level of
12 data that they would need to necessarily know that
13 the disease is spread in a particular area. But
14 if the searching were to happen in the source data
15 with the full resolution of the data, then they
16 might be able to perform better healthcare
17 analysis.

18 Q So your answer seems to assume that the
19 aggregation of data is somehow disseminated.

20 But those list of fields that should be
21 taken out under HIPAA are -- or I should say apply
22 to data that can be disseminated, correct?

1 A In order to share data.

2 Q So if the data is being aggregated --

3 MR. STEPHENS: I'm not sure if you
4 registered my objection to the last question.

5 Objection, form.

6 THE WITNESS: I'm sorry, I lost audio.
7 Can you guys hear me?

8 MR. OLIVER: Yes, we can. Can you hear
9 us?

10 THE WITNESS: I can hear you. Can you
11 guys say something?

12 MR. STEPHENS: Testing.

13 THE WITNESS: Hello.

14 MR. STEPHENS: We can hear you.

15 THE REPORTER: Do we want to go off the
16 record?

17 MR. OLIVER: Sure.

18 (Whereupon a break was had.)

19 BY MR. OLIVER:

20 Q So your answer seemed to assume that the
21 aggregation of data is disseminated.

22 A covered entity, for instance, could

1 aggregate data in a database and maintain it in a
2 high resolution form, correct?

3 MR. STEPHENS: Objection, form.

4 A So the question is whether a -- say a
5 physician's office that's covered and
6 has -- that's covered by HIPAA and has patient
7 records could aggregate -- if by aggregate you
8 mean share it with -- with someone else,
9 then -- then they would need to comply with HIPAA.
10 If you mean aggregate it in their own office on
11 their own servers and not ever share it, then I
12 suppose they wouldn't have to de-identify it.

13 Q And just to be clear, when I say
14 "aggregate," I'm basically saying taking different
15 records and putting them together in one database.

16 If it's a covered entity and that database
17 is not being shared, the records could be
18 aggregated by a covered entity and maintained at a
19 high resolution, correct?

20 MR. STEPHENS: Objection, form.

21 A When you say aggregated -- when I hear
22 "aggregated" I think of data coming from different

1 sources and being put together, and so if it's
2 coming from different sources, then it's being
3 shared, then it would be subject to HIPAA.

4 Q Let's assume there are different doctors
5 within one hospital, all of those would be covered
6 entities, correct?

7 A Yes.

8 Q And they could aggregate the various files
9 that they have into one database, correct?

10 A They could do that.

11 Q And that would not be a HIPAA violation?

12 A That is a question I would -- I would want
13 to look into and I wouldn't answer off the top of
14 my head.

15 Q If those parties were to aggregate their
16 records into one database, it could be maintained
17 in a high-resolution form so long as it was not
18 shared with a noncovered entity, correct?

19 A I -- I would need to --

20 MR. STEPHENS: Objection, form.

21 A Are you still asking with relation to
22 HIPAA?

1 Q Yes.

2 A Yeah. I -- I don't like to answer
3 questions about whether things are HIPAA compliant
4 or not without doing some research, so I would
5 need to look into that.

6 Q Okay.

7 MR. OLIVER: We've been going for about an
8 hour, so let's go off the record.

9 (Whereupon a break was had.)

10 BY MR. OLIVER:

11 Q Dr. Rubin, can you turn to Evenhaim at
12 column 8 starting around line 30?

13 A Okay.

14 Q And there it states that: The aggregator
15 may accept a query that includes lots of identity
16 specifics including a list of names or a
17 combination of a few fields that together can
18 allow identification.

19 Do you see that?

20 A I see that.

21 Q From the POSA's perspective, what would be
22 the types of fields that together could allow for

1 identification?

2 A So this could be something like birthday,
3 ZIP code, and a condition where there would only
4 be one person that would satisfy values for that.

5 Q And later in that same column,
6 specifically column 8, line 41, it again refers to
7 the parameter list and it refers to the inclusion
8 of specific individuals by name or ID or the like.

9 Do you see that?

10 A Yes.

11 Q So what would be examples of IDs for
12 individuals?

13 A It could be like a social security number.

14 Q What are other types of IDs that could be
15 used?

16 A It could be a patient number with respect
17 to a particular physician's office.

18 Q It also says: Or the like.

19 What would be "or the like" in that case?

20 A Similar things.

21 Q Can you turn to Evenhaim at column 13,
22 specifically line 33?

1 A Okay.

2 Q And that paragraph from lines 33 through
3 43 refers to transmitting of data and that the
4 steps of transmitting of data may include
5 encryption and decryption.

6 Do you see that?

7 A Yes.

8 Q And it goes on to state that: The nature
9 and quality of the security aspect is well
10 understood by the system administrator.

11 Do you see that?

12 A Yes.

13 Q What would be understood with respect to
14 encryption and decryption in transmitting data?

15 A So there are standard protocols like SSH,
16 SSL, IPsec that are used to encrypt data for
17 transmission and they perform encryption and
18 decryption.

19 Q If you could look at Evenhaim column 14,
20 lines 3 through 7.

21 You see that section?

22 A Yes.

1 Q And there it indicates that: Regardless
2 of the general level of encryption elected, a
3 parameter list including individual should carry a
4 stronger level of encryption.

5 Do you see that?

6 A I see that.

7 Q So this seems to be suggesting that the
8 transmission encryption and the parameter list
9 encryption would likely be different; is that
10 fair?

11 A Let me -- let me read the paragraph for
12 context.

13 So I think what this is suggesting to a
14 POSA is that the transmission security is not
15 necessarily enough because you have to -- it
16 doesn't protect against issues of the end point.
17 So in sending data that contains individual
18 information that has -- that is subject to
19 regulation you would want to use, you know,
20 perhaps more encryption or more security.

21 Q And when you say issues at the end point,
22 what are you referring to?

1 A The computer that receives -- so a
2 transmission has a source and a destination. So
3 the protocols that I mention, they only protect
4 the pipe, but they don't protect the destination,
5 for example. So you might want to encrypt to
6 protect the data at the destination.

7 Q And when you say protect the data at the
8 destination, what specifically do you mean?

9 A The recipient of the transmission.

10 Q Meaning the recipient of the transmission
11 would be able to decrypt the transmission but not
12 necessarily decrypt the -- the data for which the
13 enhanced encryption was used?

14 A Well, I don't see that Evenhaim goes into
15 that level of detail. It just says that it would
16 provide stronger encryption. And you asked me
17 what that meant and I think what they meant was
18 that because the data is sensitive that may not
19 rely solely on the transmission protocol for
20 security.

21 Q And what would be some examples of levels
22 of stronger encryption relative to that used just

1 for general transmission?

2 A Super encryption.

3 Q What's super encryption?

4 A Where you encrypt the data in -- and then
5 when it's transmitted, it gets encrypted again.
6 And then when it's received, the transmission
7 encryption is peeled off, but the super encryption
8 is not.

9 Q So the super encryption remains on the
10 recipient side?

11 A That would be an example.

12 Q So in that case to fully re-identify the
13 information on the recipient side there would be
14 two different decryption processes that would be
15 needed, correct?

16 A So in -- in the example that we just
17 discussed where you have super encryption, if you
18 wanted to get to the original data you would have
19 the transmission decryption take place and then
20 you would need to do another decryption.

21 Q Can you turn to Evenhaim column 8 starting
22 around line 47?

1 A Okay.

2 Q And the sentence there says: According to
3 some specific instant embodiments, all or part of
4 the parameter list is encrypted.

5 Do you see that?

6 A Yes.

7 Q What is meant by encrypting all or part of
8 a parameter list?

9 A So I would assume that that means that
10 some of the parameters are encrypted or all of the
11 parameters are encrypted.

12 Q And why would someone use one method
13 versus the other?

14 A I suppose it would depend on their
15 application and what they wanted to do.

16 Q Well, let's assume the application
17 Evenhaim where the parameter list might include a
18 list of patient names.

19 A So I think that this language is very
20 broad and it could mean that certain types of
21 fields aren't encrypted and others are, that's one
22 way to slice it. The way you said would be that

1 certain names are encrypted and others aren't, but
2 I think they just meant to say that this invention
3 includes the ability to encrypt the entire
4 parameter list or just part of it.

5 Q Can you turn to Evenhaim column 12
6 starting around line 24?

7 A Okay.

8 Q And the first sentence of that paragraph
9 indicates that: It would be appreciated that
10 there are numerous locations where an encryption
11 of an individual identification and/or merger of
12 data for individuals could be facilitated.

13 Do you see that?

14 A Yes.

15 Q What does it mean that there are numerous
16 locations where the encryption of individual
17 identification could be facilitated?

18 A So that there are -- for -- for different
19 types of -- and different purposes of encrypting
20 data you could do it in different places.

21 Q "Different places" meaning different
22 servers within the overall system?

1 A So if you read further, it's -- it talks
2 about -- one example would be to encrypt during
3 one of the substeps, so this could be in the
4 source entity processor. If merging records,
5 there could be -- it could be encrypted at the
6 aggregator.

7 Q If you turn to Evenhaim column 11 starting
8 around line 43, there's a sentence there that
9 reads: Furthermore, other variation embodiments
10 of the instant protocol are by direction, meaning
11 that the fundamental relationship between the
12 source entity and aggregator processors is
13 reversed and/or reversible.

14 Do you see that?

15 A I see that.

16 Q What does that language mean?

17 A I'm going to read for context.

18 It's saying that there could be variations
19 of the embodiment that's described where some of
20 roles that the source entity and the aggregator
21 play are reversed.

22 Q Turn back to your declaration to

1 paragraph 143.

2 A Okay. I found it.

3 Q And the title above that paragraph for the
4 heading refers to a preference in Evenhaim.

5 Do you see that?

6 A Yes.

7 Q And what do you mean by a preference?

8 A So Evenhaim -- the Evenhaim patent in the
9 abstract and throughout describes the goal of
10 searching original micro level patient data and
11 that means that because the person using such a
12 system would prefer to see high resolution, more
13 data, that's where they would perform their
14 searching.

15 Q Would it be fair to say that the person in
16 that example you just gave would be interested in
17 performing the searching on high resolution data
18 no matter where that data was located?

19 A Well, the data -- the highest resolution
20 data is going to be at the source, but if the
21 identical data were somewhere else, then I suppose
22 the search there would be equivalent.

1 Q And Evenhaim refers to preferred
2 embodiments. Can you explain the difference
3 between preferred embodiments and what the patent
4 covers as a whole?

5 MR. STEPHENS: Objection, form.

6 A When you say Evenhaim refers to preferred
7 embodiments, can you point me to what you're
8 referring to?

9 Q Sure. You can look at Evenhaim column 6,
10 line 15.

11 A Sorry. I'm in the wrong column that's
12 why. Column 6, 15.

13 So are you asking me a legal question
14 about what is the difference between a preferred
15 embodiment and other embodiments?

16 Q Well, let me ask it this way: What would
17 you understand to be the difference between a
18 preferred embodiment and what the patent might
19 encompass as a whole?

20 MR. STEPHENS: Objection, form.

21 A So I'm not a lawyer and I don't know
22 specifically what the legal implications are of

1 something being a preferred embodiment or a
2 secondary or some nonpreferred embodiments.

3 Q Generally speaking, what would a person of
4 ordinary skill understand to be the difference
5 between a preference and a requirement?

6 A A requirement is something that you have
7 to do and a preference is something that you would
8 rather do.

9 Q Can you look at Evenhaim at column 13,
10 line 33?

11 A Okay.

12 Q And in that first sentence of that
13 paragraph starting around line 35, there's the
14 term "may preferably include."

15 Do you see that?

16 A Yes.

17 Q Would a person of ordinary skill in the
18 art understand that "may preferably include" would
19 not exclude other options?

20 A I don't see that as excluding other
21 options.

22 Q Going back to column 14 of Evenhaim lines

1 3 through 7, we previously talked about that
2 stronger level encryption for the parameter list,
3 correct?

4 A Yes.

5 Q What would be the reason for using
6 stronger encryption for the parameter list?

7 A I suppose what Evenhaim's referring to
8 here is that data could be more sensitive so you
9 would want to have stronger encryption.

10 Q Let's assume as Evenhaim does that the
11 parameter list might be names of individuals for
12 which the requester is searching for healthcare
13 records.

14 In that context, what would be the reason
15 for using stronger encryption?

16 A The same answer.

17 Q And when you say the information is more
18 sensitive, sensitive with respect to HIPAA or are
19 you talking about some other more general concern?

20 A I think with respect to privacy.

21 Q Privacy in general?

22 A It would be -- it would definitely be

1 something that would be more sensitive for privacy
2 in general.

3 Q Can you turn to paragraph 109 of your
4 declaration.

5 A Okay.

6 Q And towards the bottom of page 56 in that
7 paragraph you have a citation to Evenhaim at
8 column 12, lines 16 through 20.

9 Do you see that?

10 A Yes.

11 Q And you appear to be citing that for the
12 idea that the requester should not be capable of
13 decrypting the patient-identifying information; is
14 that fair?

15 A I'm -- let me just read the paragraph.

16 Can I hear the question again?

17 Q Let me restate the question.

18 Why would it be understood to be important
19 that the requester should not be capable of
20 decrypting patient identification information?

21 A Because that would violate the
22 individual's privacy.

1 Q So is it fair to say in Evenhaim and in
2 the general understanding of a POSA that a
3 response to a query that provides healthcare
4 records of patients should be provided in a way
5 that ensures the identity of the patients cannot
6 be established?

7 A If -- if the response includes healthcare
8 information, then there should not be a -- a way
9 to identify the patient.

10 Q And would that be a POSA's understanding
11 with respect to the general requirements of HIPAA?

12 A When you say "that," you're referring to
13 my last answer?

14 Q Yes.

15 A So in HIPAA when there's a request for
16 data, the requester upon receiving the medical
17 information should not be able to identify the
18 individual. That's a requirement.

19 Q Can you turn to paragraph 118 of your
20 declaration.

21 A Okay.

22 Q You know what, I'm going to hold off on

1 that question.

2 MR. OLIVER: I said we'd take a break for
3 lunch around now, so why don't we go off the
4 record.

5 THE WITNESS: That sounds good.

6 (Whereupon a break was had.)

7 BY MR. OLIVER:

8 Q Dr. Rubin, can you turn to the Settimi
9 reference, Exhibit 1006?

10 A Okay. I've got it.

11 Q And if you could turn to paragraph 5 of
12 that reference. In the middle of that paragraph
13 there's a sentence that begins, Further,
14 information systems. Let me know when you've
15 found that.

16 A So it's, like, right in the middle?

17 Q Yes.

18 A Okay. I got it.

19 Q And that sentence reads: Further,
20 information systems may capture/retain and send
21 different levels of granularity in the data.

22 Do you see that?

1 A Yes.

2 Q And what's meant by that statement?

3 A I suppose it means that there would be
4 more detail in one information system than in the
5 other one in terms of what's captured and sent.

6 Q And the level of granularity, would that
7 be up to the designer of the system?

8 A That would make sense.

9 Q Looking at paragraph 4 of Settimi, the
10 first sentence states that: The present invention
11 generally relates to search analysis of electronic
12 medical record data.

13 Do you see that?

14 A Yes.

15 Q And what would a person of ordinary skill
16 understand to be encompassed by the concept of
17 searching medical record data?

18 A That there is something that is being
19 looked for and the place it's being looked is in a
20 database that has medical records in it.

21 Q And then in that same paragraph Settimi
22 goes on to state that: The present

1 invention -- well, let me come back to that.

2 If you could turn to paragraph 15.

3 A Okay.

4 Q There Settimi states: Certain embodiments
5 provide systems and methods for searching
6 electronic medical data to identify a pool of
7 potential study participants.

8 Do you see that?

9 A Yes.

10 Q And what would your understanding there be
11 of certain embodiments?

12 A Different examples of systems that
13 are -- are being described here.

14 Q If you could turn to paragraph 48 of
15 Settimi.

16 A Okay.

17 Q And four lines down into that paragraph,
18 there's a reference to patient-level information.

19 Do you see that?

20 A Yes.

21 Q What would a POSA understand to be
22 patient-level information?

1 A It's information about the patient.

2 Q So as an example, patient-level
3 information for a particular patient might be the
4 information contained in that patient's medical
5 record?

6 A Yes.

7 Q Can you turn to paragraph 7 of Settimi.

8 A Okay.

9 Q And the last sentence of that paragraph
10 states: To realize a full benefit of medical
11 technological growth it would be highly desirable
12 for clinical information to be organized and
13 standardized.

14 Do you see that?

15 A Yes.

16 Q And how would that statement be understood
17 by a POSA?

18 A That in order to fully utilize the growth
19 in medical technologies, it would be -- it would
20 be good for information that's clinical to follow
21 certain standardization.

22 Q And what's an example of standardization

1 in medical records?

2 A You could look at maybe HL7.

3 Q What's HL7?

4 A It's a medical record communication
5 protocol.

6 Q And what types of standardizations does
7 that protocol set forth?

8 A I have not looked at that in a while, but
9 it describes protocols for sharing medical records
10 across different institutions.

11 Q Would an example of that be that the
12 different institutions use the same terminology
13 for particular conditions?

14 A I think that would be useful.

15 Q How long has the HL7 protocol been around?

16 A I don't know, but I believe it's quite
17 old.

18 Q And would that protocol have provided
19 mechanisms for ensuring that different caregivers
20 used similar terminology in patient records?

21 A I'm not sure. I think it was more about
22 how the records are logically organized from a

1 networking perspective.

2 Q So that would be the organization part of
3 that sentence we looked at in paragraph 7,
4 correct?

5 A Well, actually, I think it would be more
6 of the standardized, because what happened is when
7 HL7 -- HL7 was introduced so that different
8 medical records companies -- different
9 organizations that shared or utilized or
10 transmitted or received medical records would have
11 a -- a, you know, kind of protocol that they could
12 use.

13 Q And what would be examples of different
14 organizations that shared medical records?

15 A Like -- I don't remember what they're
16 called, but there were organizations -- there were
17 these independent organizations that were set up
18 to allow patients to see multiple providers and
19 have those records shared. So, like, if I were to
20 go to an orthopedist, my primary care provider
21 could receive the records that were produced
22 from -- from the orthopedist.

1 Q And that independent organization would
2 sort of collect and store those records or would
3 it just be a sharing protocol?

4 A I don't remember.

5 Q Would it likely be one of those options?

6 A I think it would facilitate the
7 transmission, but I don't know if they stored
8 records.

9 Q As far as standardization, could that also
10 include the standardization of vocabulary that's
11 used?

12 A I think that makes sense.

13 Q Can you turn to paragraph 27 of Settimi,
14 please.

15 A Okay.

16 Q And the beginning of 27, Settimi appears
17 to be describing the sending of de-identified
18 patient information to a data warehouse system.

19 Do you see that?

20 A Yes.

21 Q And that data warehouse system would
22 collect and store records from various sources,

1 correct?

2 A So the question is if the patient data is
3 collected and stored in a warehouse?

4 Q From different sources, yes.

5 A Yes.

6 Q And paragraph 27 describes that this would
7 be done in a manner compliant with HIPAA; is that
8 fair?

9 A It said it would do it in a way as defined
10 by HIPAA.

11 Q So that central database would have
12 patient-level records, but it wouldn't have the
13 identifying information for the patients, correct?

14 A That sounds right.

15 Q Can you look at paragraph 38 of Settimi?

16 A Okay.

17 Q And in that paragraph, specifically in the
18 second half, there's a reference to what are
19 called patient identifiers that Settimi calls PIDs
20 and encoded patient identifiers which Settimi
21 calls EPIDs.

22 Can you explain your understanding of

1 those two concepts as used in Settimi?

2 A So looking at the end of paragraph 38, and
3 it describes the PID: To uniquely identify an
4 individual patient, and the EPID is used to
5 de-identify the patient information and then is
6 sent along with the -- with the data to the
7 warehouse.

8 Q Would an EPID be a type of token?

9 A Yes.

10 Q So the data warehouse would have, for
11 instance, a patient record and the name of the
12 patient or other identifying information be
13 removed and replaced with the EPID, correct?

14 A It doesn't say it's exactly replaced, but
15 it takes out the name and other identifying
16 information and it sends that record with the
17 EPID.

18 Q So that central warehouse could not be
19 searched using, for instance, a patient's name
20 because the data in that warehouse wouldn't have
21 patient names, correct?

22 A That's correct.

1 Q At the beginning of paragraph 38 of
2 Settimi, specifically in the second sentence,
3 there's a reference to performing the
4 de-identification process while still retaining
5 clinically useful information about the patient.

6 Do you see that?

7 A Yes.

8 Q What would be understood to be clinically
9 useful information about the patient?

10 A For example, medications that they're on.

11 Q Could that also include an ailment that
12 they're suffering from?

13 A It could.

14 Q Looking at paragraph 41 of Settimi, in the
15 first two sentences there's a discussion of EPIDs
16 and PIDs where Settimi indicates that: The
17 mapping between the two is not maintained
18 persistently.

19 Do you see that?

20 A Yes.

21 Q And what would that be understood to mean?

22 A It means that you can't go backwards from

1 the EPID to the PID.

2 Q And how would that be accomplished
3 typically?

4 A Well, you could take the PID and use the
5 one-way function on it to obtain the EPID and then
6 not store the EPID to PID mappings.

7 Q And farther down in paragraph 41 around
8 the middle there's a reference to a Twofish
9 algorithm?

10 A Yes.

11 Q Can you explain what a Twofish algorithm
12 is.

13 A Yeah. So I believe Twofish was one of the
14 AES candidates. When NIST held a competition to
15 create the next encryption standard, they got
16 submissions, I think there were 16 that were
17 chosen as finalists, and Twofish was created by a
18 cryptographer named Bruce Schneier and made it
19 pretty far along in the selection process, but
20 ultimately was not selected. So it's just a
21 symmetric block cypher.

22 Q And towards the end of paragraph 41

1 there's a discussion of other methods of creating
2 other EPIDs from PIDs. And as an example, Settimi
3 gives an algorithm based on the patient name, age,
4 and social security number.

5 Do you see that?

6 A In which paragraph?

7 Q Still in 41, in the last sentence of
8 paragraph 41.

9 A Okay. I see.

10 Q What would the understanding be of using
11 an algorithm to create an EPID that would be based
12 on, for instance, patient name, age, and social
13 security number?

14 A What's the question about?

15 Q What would a POSA's understanding be of
16 that description of the type of algorithm referred
17 to?

18 A Right. So RSA is a well-known public-key
19 algorithm. And the thing that is being suggested
20 here is that the patient's name, age, and social
21 security number have an RSA function applied to
22 it.

1 Q And is the idea that the EPID created from
2 that would be indicative of not only the person's
3 name, but also account for their age and social
4 security number and parts thereof?

5 A It's not that would be indicative of them,
6 it's that it would have been derived from them.

7 Q And what's the reason for using that type
8 of algorithm in a system?

9 A So that if the same patient is coming
10 from -- data is coming from somewhere else, it
11 will map to the same EPID.

12 Q Would it also avoid situations where two
13 patients have the same name, and therefore an EPID
14 created using this type of algorithm would avoid
15 them being mistaken for the same person?

16 A Yes. If -- if they had any difference in
17 any of the three items, then you would get a
18 different EPID.

19 Q If you could turn to paragraph 50 of
20 Settimi.

21 A Okay.

22 Q The first sentence there states that: A

1 broader analysis of patient information may be
2 allowed while at the same time respecting patient
3 privacy.

4 Do you see that?

5 A I see that.

6 Q And what would the understanding of that
7 statement be?

8 A I need to read some surrounding text.

9 So in the context of the paragraph before
10 it, the idea is that if there's information about
11 a population, analysis can be performed on that
12 population and that would not reveal anything
13 about the specific individuals in that population.

14 Q So would a broader analysis encompass
15 different types of queries?

16 A So this patent is about identifying
17 candidates for a critical study and so if, for
18 example, a query said, you know, show me everybody
19 who has diabetes in a particular area or with a
20 particular age or something like that, it might be
21 possible to identify the right group for that
22 study and perform analysis on that population

1 without performing any analysis on any individual
2 patient.

3 Q Could one perform a search in Settimi's
4 system to look for the medical records of
5 particular patients by searching by the EPIDs?

6 A I don't believe that's described in here.
7 If it is, you can show me, but my understanding is
8 that the searching in Settimi is looking for
9 patients that meet certain criteria and then
10 returning those patients and not searching on the
11 patients themselves.

12 Q Can you look at paragraph 51. And the
13 first sentence of that paragraph states: Certain
14 embodiments allow for patient information to be
15 shared with interested parties without
16 compromising patient privacy.

17 A Yes.

18 Q How would information from the data
19 warehouse and Settimi be used to share information
20 without compromising patient privacy?

21 A Well, the information in the warehouse is
22 anonymized, so -- or at least de-identified, and

1 so that could be shared without compromising the
2 identity of the patient.

3 Q Can you turn to paragraph 30 of Settimi?

4 A Okay.

5 Q And the second sentence of that paragraph
6 means -- excuse me, the second sentence of that
7 paragraph reads: In an exemplary embodiment of
8 present invention endusers may include PCP staff
9 members, pharmaceutical company research members,
10 and personnel from companies that make medical
11 and/or other products.

12 Do you see that?

13 A Yes.

14 Q And what would you understand to be
15 companies that make medical and/or other products
16 to mean in this paragraph of Settimi?

17 A So, for example, let's say you have a
18 company that makes an infusion pump. That company
19 may have a research team and want to get medical
20 information, so that would be the example.

21 Q Are there other examples of companies or
22 limitations on companies that you can think of?

1 A I mean, my company Harbor Labs works with
2 dozens of medical device manufacturers. Any one
3 of them would qualify for this.

4 Q It wouldn't necessarily be limited to
5 device manufacturers, though, correct?

6 A The language says: Medical -- that make
7 medical and/or other products. So that could
8 be -- that's very broad, I guess.

9 Q Can you turn to paragraph 141 of your
10 declaration, please?

11 A Okay.

12 Q And on page 78 within paragraph 141, you
13 refer to common vocabulary that normalizes
14 terminology in the data from multiple sources.

15 Do you see that?

16 A Yes.

17 Q And what's the meaning of common
18 vocabulary as you use it here?

19 A I'm going to pull up a searchable copy of
20 Settimi. So vocabulary is -- refers to the syntax
21 that's used for performing queries.

22 Q And can you provide an example of that?

1 A Paragraph 60 of Settimi, it says -- it
2 talks about the common vocabulary and then it
3 says: For example, if one record refers to MI and
4 another record refers to myocardial infarction,
5 both are coded centrally in the database as a
6 myocardial infarc.

7 Q And what would be a reason that one would
8 want to use a common vocabulary for data stored in
9 a central data warehouse?

10 A Says it makes it more -- the searching
11 more accurate, because if you wanted to search for
12 people, for example, that had the condition of
13 myocardial infarction and you didn't have a common
14 vocabulary you might miss the ones that are MI
15 versus the ones that have the full name in it.

16 Q So, for instance, one healthcare provider
17 at one data source might only use the term MI,
18 where a healthcare provider in charge of another
19 data source might use different terminology?

20 A I think that's an example of why it would
21 be helpful to have a common vocabulary.

22 Q And both in paragraph -- the section of

1 paragraph 141 of your declaration that we
2 discussed and in paragraph 60 of Settimi which you
3 just raised, there's the term "normalized."

4 And what's the meaning of normalizing data
5 in connection with this discussion of common
6 vocabulary that we've had?

7 A So the -- the idea is to take things that
8 really mean the same thing, like MI and the
9 myocardial thing and replace them with just one
10 thing that's common so everyone is using the same
11 term.

12 Q In paragraph 66 of Settimi, let me know
13 when you're there.

14 A Yeah. One second. I need to crack a
15 window open and take my jacket off. It's really
16 hot in here.

17 Q No problem.

18 A Secret revealed. Should have turned off
19 the camera.

20 Q Paragraph 66.

21 A Yes.

22 Q At the end of that paragraph, I guess five

1 lines up from the bottom it says: Normalized or
2 codified.

3 Do you see that?

4 A Yes.

5 Q What's the difference between normalizing
6 data and codifying it?

7 A So normalizing is a way of codifying.
8 Codifying is a broader term.

9 Q And what would codifying encompass that
10 normalizing wouldn't?

11 A Well, codifying could refer to other
12 things. For example, you could take a whole bunch
13 of different procedures like the one we talked
14 about earlier with the long name and give them a
15 code. Like, you could say, this is an MI, and so
16 if you attach different codes to different sets of
17 words and then everybody uses them, then you'll be
18 able to have a common vocabulary.

19 Q And in paragraph 66, which we've been
20 discussing, the normalization here is with respect
21 to the search criteria, correct?

22 A In this particular location it's talking

1 about normalizing the search criteria.

2 Q So normalization could take place when
3 uploading files to a central warehouse and it
4 could also take place when receiving a query that
5 would search for certain elements within that
6 database, correct?

7 MR. STEPHENS: Objection, form.

8 A So I don't know that this reference
9 discloses that, but in general, you can normalize
10 data when you receive it or when you query it.

11 Q Just to be clear though, you agree that 66
12 is talking about normalization with respect to the
13 query, correct?

14 A That -- that's what's described here in
15 this section you pointed me to.

16 Q If you turn to paragraph 73 of Settimi.

17 A Okay.

18 Q About six lines down in that paragraph
19 Settimi states: Alternatively, terms may be
20 selected and/or entered without regard to a
21 particular vocabulary.

22 Do you see that?

1 A I see that.

2 Q And what would that mean?

3 A I'm sorry?

4 Q What does that mean?

5 A This is saying that alternatively there
6 can be queries that are not normalized, they're
7 just whatever the requester asked.

8 Q So the query could be the requester
9 saying, I want this specific thing and there's no
10 normalization of whatever that query term is?

11 A So this text is saying that it could
12 also -- in addition to what was described earlier,
13 there could just be a request that doesn't get
14 normalized.

15 Q And what would be a reason for doing that?

16 A I suppose that the authors wanted the
17 flexibility -- or the applicant, I should say,
18 wanted the flexibility of being able to send
19 queries without having them normalized.

20 Q Can you turn to paragraph 119 of your
21 declaration?

22 A Okay.

1 Q And in the last sentence of paragraph 119,
2 you use the term "teaches away"?

3 A Right.

4 Q And what's your understanding of the term
5 "teaches away"?

6 A That it discloses something that's at odds
7 with the other thing. So it teaches away from it.

8 Q What do you mean by discloses something
9 that's at odds?

10 A So it's basically teaching something that
11 would -- would be the opposite or would sort of
12 take one in a different direction from the thing
13 that you're teaching away from.

14 Q And in what manner do you think Evenhaim
15 teaches away from what's being discussed in
16 paragraph 119?

17 A I need to read it now.

18 So the -- the Evenhaim reference teaches
19 matching in the source entities and that happens
20 before there's any de-identification, and so that
21 teaches away from the approach of the '641 patent
22 which is to -- to match tokens that have already

1 been de-identified.

2 Q Can you turn to the Dick reference,
3 Exhibit 1007?

4 A Okay.

5 Q And if you could turn to paragraph 45 of
6 that reference.

7 A Okay.

8 Q And there's a discussion in paragraph 45
9 of de-identifying records.

10 Can you tell me if there's any specific
11 methods of de-identification that would be
12 required by paragraph 45?

13 A So paragraph 45 describes removing certain
14 identifying information and it gives a list of
15 things. And it also says that if that process
16 were to be useless, one could consult with an
17 appropriate person with knowledge and experience
18 to de-identify.

19 Q But it says to consult with the
20 appropriate person with knowledge and experience.

21 Is that for the purpose of the particular
22 mechanism for de-identifying?

1 A It's to make sure that whatever method was
2 used properly de-identifies.

3 Q And what would be some examples of methods
4 that could be used to de-identify?

5 A One is described here of stripping out
6 certain fields from the records.

7 Q Well, I guess my question is more: Isn't
8 de-identifying removing identifying information?

9 A That's right.

10 Q And isn't sort of stripping out the
11 information the definition of de-identification
12 more or less?

13 A Well, there's -- there's more to it.
14 Like, the idea that certain combinations of
15 information or certain patterns of queries could
16 be used to reidentify. So there's more than just
17 stripping out.

18 Q Prior to 2009, what would have been known
19 methods of de-identifying medical records? And
20 I'm talking about the specific system designs or
21 process designs.

22 A I -- I can't think of that off the top of

1 my head and I don't believe it's in my
2 declaration, so...

3 Q Does paragraph 45 sort of provide a
4 specific system design or process design for
5 de-identification?

6 A Yes.

7 Q And what's that?

8 A To strip out the information that's listed
9 in that paragraph and then if some of it is to not
10 be taken out, then making sure that an expert with
11 the right knowledge and experience approves that
12 it's still de-identifying.

13 Q So what's the difference then between just
14 the definition of de-identification and stripping
15 out identifying information?

16 A I'd have to think about that. I don't
17 have an opinion on that in my declaration.

18 Q What's the specific manner of stripping
19 out information described in paragraph 45?

20 A It's -- it talks about removing those
21 fields.

22 Q Well, aren't there different ways to

1 remove information?

2 A I suppose you could override it with zeros
3 or you could override it with 1s, that would be
4 different. But in general, you make sure those
5 fields no longer have the information that you're
6 stripping out.

7 Q Can you look at paragraph 46 of Dick?

8 A Okay.

9 Q And in the first sentence there, it refers
10 to de-identifying methods and processes.

11 A Right.

12 Q What's encompassed in de-identifying
13 methods and processes?

14 A It's ways of de-identifying records so
15 that they can be used for medical research.

16 Q Were there at the time different methods
17 and processes known?

18 A Yes.

19 Q And what different methods or processes
20 would a person of ordinary skill think of when
21 reading paragraph 46 of Dick?

22 A I would need to go back and do some

1 research. I didn't opine on this in my report.

2 Q Can you turn to paragraph 24 of Dick?

3 A Okay.

4 Q And paragraph 24 discusses a request that
5 includes identification of a subject, correct?

6 A Yes.

7 Q And the subject might consist of a human
8 individual or a group of humans, correct?

9 A Yes.

10 Q So the search request in Dick could be a
11 list of particular patients; is that fair?

12 A Yes.

13 Q If you'll look at paragraph 3 of Dick,
14 please.

15 A Okay.

16 Q It says in the second sentence of that
17 paragraph that: Many fields of insurance such as
18 life and health routinely require medical
19 information for analysis.

20 Do you see that?

21 A Yes.

22 Q And why is that?

1 A Well, for example, if you're going to get
2 life insurance, the insurance company would want
3 to know if you have conditions that could cause
4 you to have an early death.

5 Q So it would be for the purpose of
6 determining the risk of selling different
7 insurance products such as life insurance or
8 long-term care insurance; is that fair?

9 A That -- those are -- that's an example.

10 Q MR. OLIVER: We've been going for about an
11 hour. Why don't we go off the record and take a
12 break.

13 (Whereupon a break was had.)

14 BY MR. OLIVER:

15 Q Dr. Rubin, can you turn to the Landi
16 reference, Exhibit 1008?

17 A Okay.

18 Q Can you turn to column 8 of Landi starting
19 at line 38?

20 A Okay.

21 Q And in that paragraph around line 47
22 there's a reference to: Public keys are freely

1 distributable, and then a parenthetical statement
2 that says: No HIPAA issues.

3 Do you see that?

4 A I see that.

5 Q Do you have any reason to disagree with
6 the statement there of, no HIPAA issues?

7 A Let me read the whole paragraph. So it's
8 saying that the public keys are freely
9 distributable to healthcare organizations for
10 de-identification of patient data and in
11 parentheses it says: No HIPAA issues in the
12 middle.

13 And you're asking me if I agree that there
14 are no HIPAA issues?

15 Q I guess more specifically do you think
16 Landi is wrong in its characterization --

17 MR. STEPHENS: Objection, form.

18 I'm sorry. Go ahead.

19 Q -- as to whether or not there are HIPAA
20 issues?

21 MR. STEPHENS: Objection, form.

22 A I think that when dealing with -- with

1 medical information, there are always HIPAA
2 issues, even some which is, if we're talking about
3 public keys, how are the private keys protected,
4 what algorithms are being used, what key lengths,
5 who has access to them. So I wouldn't
6 characterize that as no HIPAA issues.

7 Q Do you see any HIPAA violation in what's
8 described in that paragraph?

9 A I would need to review this in the context
10 of HIPAA. For example, we talked about whether
11 re -- the ability to reidentify patients is
12 consistent with HIPAA, and my answer was that I
13 need to look at that and research it, I can't
14 answer that off the top of my head. So that's the
15 same answer to that here.

16 Q Can you take a look at Landi at column 2,
17 line 41?

18 A Okay.

19 Q And there's a discussion in that paragraph
20 extending from column 2, line 41 through line 53.

21 Do you see that?

22 A Yes.

1 Q Let me know if you can spot or if you
2 believe there's any HIPAA violation in what's
3 described in that paragraph.

4 A So my understanding of HIPAA is that there
5 should be no way to reidentify the de-identified
6 data, but as to whether this specific description
7 is in the HIPAA violation, I would require more
8 research.

9 Q Have you performed any analysis as to
10 whether or not the embodiments and operations
11 described in Landi constitute a HIPAA violation?

12 MR. STEPHENS: Counsel, are there specific
13 embodiments or examples you'd like to direct Dr.
14 Rubin to?

15 MR. OLIVER: I'm just asking whether he's
16 performed that analysis for any part of Landi.

17 A I'm going to search my report. Yes, in
18 paragraph 171 on page 95 of my declaration.

19 Q And what specifically in paragraph 171 are
20 you referring to?

21 A So it's -- I say that: This proposed
22 method of de-identification is not compliant with

1 HIPAA.

2 Q And what's your basis for that position?

3 A So I give three -- three basis. It does
4 not meet the de-identification standards, it does
5 not meet the re-identification requirements, and
6 it does not meet the requirement establishing the
7 standard for de-identified data, and then I kind
8 of summarize each of those.

9 Q If a data source such as doctor's office
10 were to de-identify a patient record to be
11 compliant with HIPAA such that no identification
12 information remained and the doctor's office then
13 destroyed the key that was used to de-identify,
14 would that de-identified record be shared with
15 others under HIPAA?

16 A It depends.

17 Q And why is that?

18 A Because there's third the requirement of
19 making sure there's no reasonable basis to believe
20 the information could be used to identify an
21 individual.

22 Q The doctor's office would always have the

1 original patient records, correct?

2 A Correct.

3 Q Not always. The doctor's office that
4 creates the de-identified record would also have
5 the original record, correct?

6 A Most likely.

7 Q So that doctor's office could always
8 identify what the de-identified record corresponds
9 to just by matching the two of those, correct?

10 A The doctor already has the non
11 de-identified records, so they would know.

12 Q So in that sense it would be reversible by
13 at least the doctor, correct?

14 A I was talking about reason 3, which did
15 not have to do with reversing; it had to do with
16 that there's no way that this information couldn't
17 be, for example, combined with other information
18 to identify it by the party to whom the
19 de-identified data was sent.

20 Q Well, let's keep with the reversible part
21 then.

22 A Okay.

1 Q In that case, the doctor could always
2 reverse it, right?

3 A They wouldn't need to reverse it, they
4 would already have it.

5 Q But they could. Basically if they
6 de-identified a bunch of records, they could then
7 figure out which one of those records corresponds
8 to which patient because they had the original
9 records, correct?

10 A That would be silly. They wouldn't need
11 to do that, they already have the records.

12 Q If that's the case why would the doctor's
13 office need to destroy the key that could
14 reidentify the records if the doctor's office
15 could do it anyway?

16 A So I -- I don't know that you can digest
17 the HIPAA rule down to destroy the key. I think
18 it's a lot more involved than that. Destroying
19 the key may be one way to do it, but the HIPAA
20 rules are -- they have a specific explanation of
21 when you shouldn't be able to reidentify.

22 Q If a doctor's office used a public

1 private -- let's say the doctor's office used some
2 sort of encryption key and the doctor's office
3 never shared the key that would allow for
4 re-identification, would that be a HIPAA violation
5 by the doctor's office since the doctor's office
6 already knows whose records belong to whom?

7 MR. STEPHENS: Objection, form; scope.

8 A I can't do HIPAA compliance analysis on
9 the fly. That's an involved process.

10 Q You would agree, though, that some
11 entities such as the doctor's office that
12 performed the de-identification could always
13 re-identify by matching up the de-identified
14 record and the original record, correct?

15 A Again, that's -- I wouldn't put it that
16 way because I think the doctor doesn't need to
17 reidentify, they already have the records, so
18 there's no need for them to reverse anything.

19 Q But they could do it if they wanted to?

20 A I don't think it makes sense to ask them
21 to do it. You have the original record, then you
22 have the de-identified record and so you still

1 have the original if you haven't deleted it.

2 Q I'm not asking whether or not someone's
3 requesting that they do it.

4 I'm just asking whether it's statistically
5 possible that the doctor's office having the
6 original records and the de-identified records
7 could pair them back up and figure out, you know,
8 which patient belongs to which de-identified
9 record?

10 A It may or it may not be depending on if
11 you -- -- if you de-identified a bunch of records
12 and resulted in -- for different patients and it
13 resulted in the same output, then you may not
14 know -- so here's a counterexample.

15 Say you have five patients and you
16 de-identified all of them and then you threw out
17 four of those records and you're left with just
18 one of the records and there's no identifying
19 information and everything else in the records are
20 the same. So you wouldn't have any way to reverse
21 it and go back to the one that you started from.

22 Q Your hypothetical assumes that every

1 single patient record that was de-identified has
2 the same health information; is that correct?

3 A Well, you asked me in general if a doctor
4 would be able to reverse it and I showed you a
5 counterexample. I mean, so I don't think there's
6 a general rule for whether or not you can do that.

7 Q Let me be more specific in my example
8 then.

9 There are five patient records held by a
10 doctor's office. Each of those patients is
11 different ages, has different birthdays, has
12 different medical conditions, and has been
13 prescribed different medications. The doctor
14 performs a de-identification of those records
15 using an encryption method. And the doctor's
16 office holds the key to reidentify or undo the
17 encryption.

18 Do you understand that hypothetical I've
19 set forth?

20 A Yes.

21 Q Now, in that situation if the doctor has
22 the records that have been de-identified and the

1 records that were the original ones, could the
2 doctor figure out which de-identified record
3 corresponds to which patient by simply comparing
4 the two different versions?

5 A So in the very specific example that you
6 just gave, assuming that none of the health
7 information that's unique to all the patients had
8 to be removed as part of de-identification, then
9 the doctor should be able to correlate the
10 de-identified records to the original records.

11 Q So in that case there could be a
12 re-identification?

13 A In the very specific case that you just
14 gave where a doctor has all the originals and the
15 de-identified has health information in it that
16 matches the originals and doesn't match any other
17 one and there's a correlation there in that
18 example, that would allow the doctor to know which
19 ones go with which ones.

20 Q And that would be a type of
21 re-identification?

22 A Well, it would be a way for the doctor to

1 see which of the de-identified records that have
2 certain health information that's very specific to
3 the original records came from which of the
4 original records.

5 Q Is that a violation under HIPAA?

6 A I don't -- I can't do HIPAA compliance
7 analysis on the fly. I would need to research
8 that.

9 Q Can you turn to Landi at column 3 starting
10 around line 52?

11 A Okay.

12 Q And the sentence there says:
13 Advantageously as explained below, systems and
14 methods according to the invention for
15 de-identifying/re-identifying patient data can be
16 implemented for various purposes such as research,
17 public health, or healthcare operations while
18 maintaining compliance with regulations based on
19 HIPAA for protecting patient privacy.

20 Do you see that?

21 A Yes.

22 Q Is it your position that Landi is simply

1 wrong concerning HIPAA requirements?

2 A I'm going to go into my report. I have a
3 section in my report I mentioned a minute ago that
4 Landi's method of de-identification does not
5 satisfy HIPAA. And with respect to your specific
6 sentence that you just asked about, I would have
7 to do further research and analysis to answer that
8 question.

9 Q Well, just so we're on the same page, do
10 you agree that the sentence in Landi we just
11 discussed at column 3 starting around line 52
12 talks about de-identification and
13 re-identification of patient data while
14 maintaining compliance with HIPAA, correct?

15 A It talks about that. As to whether I
16 believe that that is correct is something I would
17 have to do more research on.

18 Q But would you agree that that statement
19 indicates that Landi's intention in connection
20 with the systems and methods of the invention
21 described in that patent are intended to comply
22 with HIPAA?

1 A I can't speak for the inventors'
2 intention. They may have thought that they were
3 compliant, but I can't speak to what their
4 intentions were.

5 Q Let me ask it a different way: Would a
6 person of ordinary skill in the art reading that
7 sentence understand it to indicate that the
8 systems and methods described in Landi were
9 intended to comply with HIPAA?

10 A I think a POSA would read this and
11 understand that the inventors thought that they
12 were designing something that was compliant with
13 HIPAA.

14 Q And your opinion in your declaration is
15 that Landi's method of de-identification does not
16 satisfy HIPAA, correct?

17 A Yes.

18 Q So you disagree with the disclosure of
19 Landi at least with respect to whether or not it
20 complies with HIPAA?

21 A I would have to look to see whether Landi
22 claims that its method of de-identification is

1 HIPAA compliant.

2 Q Do you think its method of
3 de-identification is HIPAA compliant?

4 A No.

5 Q And what's the specific reason for that?

6 A So it's outlined in paragraphs 170 and
7 171. Landi describes how different healthcare
8 organizations de-identify their records by
9 creating an encrypted token and encrypted form of
10 a PII such as a name or social security number.
11 And encrypting patient identify -- so I list out
12 three requirements of HIPAA as I mentioned earlier
13 and the specific method of de-identification does
14 not satisfy those.

15 Q And what specific of those does it not
16 satisfy? Well, let me ask a specific question.

17 With respect to reproducibility, whether
18 someone could reidentify which record matched to
19 which patient, if the only entity that had the key
20 for doing so was the covered entity under HIPAA
21 such as the doctor's office, why would it matter
22 that the doctor's office could re-identify which

1 patient matched with which healthcare record?

2 A So I -- I don't have full recollection of
3 all the insights that went into the creation of
4 HIPAA. But one reason I could think of off the
5 top of my head would be that the doctor's office
6 now has the burden of protecting that key and
7 making sure that it's never compromised. But I
8 don't specifically, you know, have the HIPAA rules
9 and -- and -- you know, memorized and I'm not
10 really sure -- you know, I would need to do more
11 research to answer that.

12 Q Is there anything in HIPAA that you're
13 aware of that would prevent the doctor from having
14 the key if it's not disseminated to a noncovered
15 entity?

16 A I can't answer that without looking
17 through the -- the HIPAA document again.

18 Q What would be the patient privacy concern
19 in a doctor who has the patient's medical records
20 from being able to re-identify medical records for
21 that same patient?

22 A I can't think of anything.

1 Q Can you turn to Landi at column 14
2 starting around line 26?

3 A Okay.

4 Q And in that section after the
5 de-identification process is complete, the records
6 are uploaded to a central data processing system,
7 correct?

8 A It doesn't use those exact words, but
9 that's what it says.

10 Q And so this is a centralized data
11 warehouse that would store de-identified patient
12 records?

13 A Right.

14 Q So in that type of system the centralized
15 data warehouse would not have, for example, names
16 of patients, correct?

17 A Correct.

18 Q And therefore, if one were to be
19 interested in looking for a particular patient's
20 records, those records couldn't be searched by
21 using the patient's name, correct?

22 A Landi does not describe that type of a

1 search, but I -- I don't think you could use the
2 name. And it wouldn't be good if you could
3 because then you could correlate that name to the
4 medical information.

5 Q If you could turn Landi at column 4, line
6 18.

7 A Okay.

8 Q And Landi uses the term "trusted broker
9 system."

10 Do you see that?

11 A Yes.

12 Q In this field, what would one understand
13 to be a "trusted broker"?

14 A We talked earlier about the trusted third
15 party. Would be the same thing.

16 Q And HIPAA provides for what are known as
17 business associates.

18 Could a business associate be a trusted
19 broker?

20 A I need to look at HIPAA again. I just
21 don't remember it well enough to answer that.

22 Q Can you look at Landi at column 5 starting

1 around line 13?

2 A Okay.

3 Q And there's a reference there to an
4 encrypted ID which is a unique reproducible
5 encrypted version of patient identifying
6 information.

7 Do you see that?

8 A Yes.

9 Q Would that be an example of a token?

10 A It could be.

11 Q Can you turn to Landi at column 11,
12 please, starting around line 52?

13 A Okay.

14 Q And in that paragraph there's a discussion
15 with replacing de-identified data elements with
16 short readable strings associated with encrypted
17 IDs.

18 Do you see that?

19 A I see that.

20 Q And what would a POSA understand to be the
21 purpose of those readable strings?

22 A I suppose one reason to do that would be

1 to make the database more readable so you could
2 put in information in the string about what type
3 of field this was before it was de-identified.

4 Q So by what type of field, it could be a
5 name field versus a date of birth field or
6 something to that extent?

7 A Right.

8 Q If you could turn to the Murphy reference,
9 Exhibit 1009, please?

10 A Okay.

11 Q In what I'll call the abstract on page 552
12 above the Introduction, if you could look at that.

13 A Okay.

14 Q In that abstract, although it's not titled
15 that, there's a discussion of obfuscation of data.
16 Can you explain what that is?

17 A So obfuscation in the way it's described
18 in this paper is a perturbation of the values so
19 that one can't see what the actual values were.

20 Q I'm sorry, what did you say it was as far
21 as values?

22 A A perturbation where that's, like, a --

1 making some kind of change to it.

2 (Reporter clarification.)

3 Q On page 552 of Murphy on the second
4 column, the last paragraph in that column refers
5 to an attack on the system.

6 Do you see that?

7 A Yes.

8 Q And what's being referred to here when the
9 term "attack" is used?

10 A So an attack is an attempt to obtain
11 information that the system is designed to prevent
12 you from obtaining.

13 Q And the example here, it seems the attack
14 is to try and perform a search for medical records
15 that would allow you to match the information to
16 one particular person; is that right?

17 A Yes.

18 Q And in that same column, Figure 1 has a
19 little description there about the query.

20 Do you see that?

21 A Yes.

22 Q And in this example the query is for the

1 number of patients matching certain criteria,
2 correct?

3 A Yes.

4 Q And the example here is the number of
5 patients that are female?

6 A Right.

7 Q And another example of this type of query
8 is provided on page 554 of Murphy at the top of
9 column 1, and the example there is about finding
10 the number of patients that have the diagnosis of
11 manic depression, correct?

12 A Yes.

13 Q And looking at page 555 of Murphy, column
14 1, the middle part of the second paragraph has a
15 sentence that begins, Our next approach.

16 Do you see that?

17 A Yes.

18 Q And in that discussion was to essentially
19 block or -- well, let me rephrase that.

20 Rather than block, it's trying to prevent
21 answering the question for the number of patients
22 if the response would answer that there were one

1 or two patients, correct?

2 A No. It will still give an answer, but
3 what it's doing is it's obfuscating the response
4 by always giving the same answer when it's in that
5 range.

6 Q And the same answer would be potentially
7 saying less than three?

8 A That -- that's the way that it describes
9 doing that for this example.

10 Q So if the person asked for the number of
11 patients with manic depression in a specific ZIP
12 code and there were only two such patients, rather
13 than saying the answer is two, it would say, less
14 than three?

15 A It would say, the answer is less than
16 three.

17 Q If you could look at page 556 of Murphy.

18 A Okay.

19 Q Column 1, the second paragraph up from the
20 bottom beginning, Acceptable.

21 A Okay.

22 Q It states that: Acceptable methods of

1 obfuscation will be dependent on the types of data
2 that need to be served back to the client
3 application.

4 Do you see that?

5 A Yes.

6 Q And what does that mean?

7 A It's saying that there are many different
8 ways that one could obfuscate and how it's done is
9 going to depend on what type of data is going to
10 be sent as a result of the request.

11 Q And if you look on page 556, column 2, in
12 that last full paragraph there it says: The data
13 obfuscation method discussed in this paper does
14 not limit the logic of the query nor the data
15 elements or values that can be used in the query.

16 Do you see that?

17 A Yes.

18 Q And what's meant by that statement?

19 A That -- they're saying that the method
20 that's described here was -- there were specific
21 examples given, but that -- those examples are not
22 limiting, it could be other things, too.

1 MR. OLIVER: We've been going for almost
2 but not quite an hour. Why don't we take a break
3 and go off the record.

4 (Whereupon a break was had.)

5 BY MR. OLIVER:

6 Q Dr. Rubin, have you had any conversations
7 about the substance of your testimony with anyone
8 during any of the breaks today?

9 A No.

10 MR. OLIVER: Thank you and I have no
11 further questions for the witness.

12 MR. STEPHENS: I'd like to take
13 15 minutes, please, so we can consider any
14 questions for redirect.

15 MR. OLIVER: All right.

16 (Whereupon a break was had.)

17 EXAMINATION

18 BY MR. STEPHENS:

19 Q I'd like to start with the Evenhaim
20 reference.

21 A Okay.

22 Q Do you recall being asked by Petitioner's

1 counsel about Evenhaim's discussion of keys in
2 columns 12 and 13 of Evenhaim?

3 A Yes.

4 Q And I'd like to look at column 12 around
5 lines 12 to 13.

6 A Okay.

7 Q And this passage refers to data sources
8 that encrypt the identifying portions of each
9 record using a common encryption key.

10 Do you see that?

11 A Yes.

12 Q What would a POSA's understanding have
13 been of a common encryption key as used in this
14 passage?

15 MR. OLIVER: Objection, scope.

16 A It would be like an AES encryption key and
17 a key that's used to encrypt data.

18 Q Then I'd like to turn to column 13.

19 And do you recall being asked about the
20 disclosure at lines 4 through 12 of column 13?

21 A Yes.

22 Q And here Evenhaim refers to: Data being

1 released from the first data source where we will
2 get both keys and healthcare data.

3 And it goes on to describe: Encrypting
4 several keys that can uniquely identify the
5 person.

6 Do you see that?

7 A Yes.

8 Q What would a POSA's understanding have
9 been of a key as used in this passage of Evenhaim?

10 A Here it's referring to, like, the
11 encrypted private information that's sent along in
12 the de-identified data.

13 Q So would a POSA have understood that the
14 term "key" as used in those two passages that we
15 just reviewed have different meanings in those
16 different contexts?

17 A Yes.

18 MR. OLIVER: Objection, leading.

19 Q I'd like to look at column 14.

20 A Okay.

21 Q Lines 4 through 7.

22 Do you recall being asked about this

1 disclosure during your cross-examination?

2 A Yes.

3 Q And this passage explains that regardless
4 of the general level of encryption elected, a
5 parameter list including individuals should carry
6 a stronger level of encryption, correct?

7 A Yes.

8 Q Does anything in this passage disclose or
9 suggest to a POSA that individuals' names would be
10 tokenized in the parameter list?

11 MR. OLIVER: Objection, leading.

12 A No.

13 Q I'd next like to refer to column 8.

14 A Okay.

15 Q And lines 47 to 48. These lines read:
16 According to some specific instant embodiments,
17 all or part of the parameter list is encrypted.

18 Did I read that correctly?

19 A Yes.

20 Q Do you recall being asked about this
21 disclosure during cross-examination?

22 A Yes.

1 Q According to this disclosure, all of the
2 parameter list can be encrypted in certain
3 embodiments; is that right?

4 MR. OLIVER: Objection, leading.

5 A Yes.

6 Q And what's the alternative disclosed here?

7 A The alternative is that part of the
8 parameter list is encrypted.

9 Q Why would Evenhaim be interested in
10 encrypting only part of the parameter list?

11 A It's possible that there may have been
12 parameters that are not security sensitive, so
13 they wouldn't need to be encrypted.

14 Q What are some examples of parameters that
15 might not be security sensitive? I'll strike that
16 question.

17 Are there examples of where Evenhaim
18 might -- well, strike that.

19 Does anything in this passage indicate
20 that a partial encryption of the parameter list
21 would involve tokenizing names of individuals?

22 MR. OLIVER: Objection, leading.

1 A No.

2 MR. STEPHENS: No further questions.

3 FURTHER EXAMINATION

4 BY MR. OLIVER:

5 Q Dr. Rubin, from the end of my questioning
6 to the start of the questioning that just began a
7 few minutes ago, did you have any discussions
8 about this case with anyone?

9 A Just with counsel.

10 Q And as counsel you're referring to
11 Mr. Stephens?

12 A Yes.

13 Q And what was the nature of that
14 discussion?

15 A We discussed --

16 MR. STEPHENS: Dr. Rubin, you don't need
17 to answer that question.

18 Objection, privilege.

19 MR. OLIVER: In that case I have no
20 further questions.

21 MR. STEPHENS: Off the record.

22 THE REPORTER: I don't believe I have

1 standing orders for anyone.

2 MR. OLIVER: That is correct. Would it be
3 possible to get a final by Wednesday of next week?

4 THE REPORTER: Yes.

5 For you, Mr. Stephens?

6 MR. STEPHENS: And we don't need an order.
7 We'll just receive the transcript when they file.

8 (Whereupon the proceedings were concluded at
9 2:32 p.m. CST)

10

11

12

13

14

15

16

17

18

19

20

21

22

1 CERTIFICATE OF SHORTHAND REPORTER - NOTARY PUBLIC

2 I, Karisa Ekenseair, Certified Reporter and
3 Notary Public within and for the State of Arkansas
4 do hereby certify: That AVIEL D. RUBIN, PHD,
5 the witness whose deposition is hereinbefore set
6 forth, was duly sworn by me before the commencement
7 of such deposition and that such deposition was
8 taken before me and is a true record of the
9 testimony given by such witness.

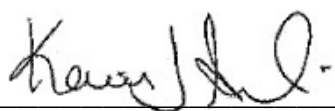
10 I further certify that the adverse party,
11 Patent Owner, was represented by counsel at
12 the deposition.

13 I further certify that the deposition of
14 AVIEL D. RUBIN, PHD, occurred virtually on
15 November 22, 2024, commencing at 8:32 a.m. to 2:32
16 p.m. CST.

17 I further certify that I am not related to any
18 of the parties to this action by blood or marriage,
19 I am not employed by or an attorney to any of the
20 parties to this action, and that I am in no
21 way interested, financially or otherwise, in the
22 outcome of this matter.

1 IN WITNESS WHEREOF, I have hereunto set my hand
2 and affixed my notarial seal this 27th day of
3 November 2024.

4 My commission expires: 6-18-2028

5
6 
7 _____

8 Karisa Ekenseair, CCR, RPR LS #802

9 Notary Public in and for

10 Pulaski County, Arkansas

11 Commission No. 12704567

12

13

14

15

16

17

18

19

20

21

22

A	140:1, 140:19, 141:22, 142:20, 144:8 above 81:3, 134:12 absent 7:5, 8:3 abstract 81:9, 134:11, 134:14 accept 72:15 acceptable 137:20, 137:22 access 23:11, 30:20, 43:13, 117:5 accessible 41:13 accomplished 97:2 according 78:2, 126:14, 142:16, 143:1 account 99:3 accurate 104:11 achieve 60:12, 60:18, 61:6, 67:14 acquires 19:18 acronym 7:21, 45:3 across 19:3, 61:8, 91:10 acting 23:21 action 146:18, 146:20 actual 134:19 actually 40:17, 46:12, 92:5 addition 108:12	address 33:11, 37:3 addressed 27:11 administrative 9:19 administrator 74:10 adopted 40:18, 44:21 advance 44:19 advantageously 126:13 adversary 43:9, 43:12 adverse 146:10 advice 13:11 aes 44:11, 44:17, 44:19, 46:20, 53:22, 54:6, 54:12, 97:14, 140:16 affect 6:17, 47:6 affixed 147:2 after 13:18, 54:14, 131:4 again 27:4, 29:21, 32:16, 36:20, 47:19, 48:17, 73:6, 77:5, 85:16, 122:15, 130:17, 132:20 against 27:17, 43:22, 44:3, 45:7, 46:3, 75:16 age 6:3, 51:2, 98:3, 98:12, 98:20, 99:3,	100:20 agent 23:21, 24:17, 24:19, 24:21, 51:21, 52:3, 52:4, 52:15 agents 52:10 ages 124:11 aggregate 66:10, 67:21, 70:1, 70:7, 70:10, 70:14, 71:8, 71:15 aggregated 64:11, 64:12, 64:15, 65:8, 65:10, 69:2, 70:18, 70:21, 70:22 aggregation 65:1, 67:7, 68:19, 69:21 aggregator 38:16, 38:20, 38:21, 39:13, 56:2, 57:21, 72:14, 80:6, 80:12, 80:20 ago 127:3, 144:7 agree 40:14, 40:15, 40:16, 59:12, 107:11, 116:13, 122:10, 127:10, 127:18 agreed 57:21, 58:4, 59:1 agreement 26:19, 30:7, 59:6 ahead 116:18 ailment 96:11
----------	--	--	--

algorithm 97:9, 97:11, 98:3, 98:11, 98:16, 98:19, 99:8, 99:14 algorithms 60:5, 117:4 all 7:7, 7:10, 8:1, 9:1, 15:3, 15:5, 16:14, 20:2, 26:6, 30:9, 39:7, 39:15, 44:13, 46:10, 46:18, 47:5, 47:7, 62:22, 71:5, 78:3, 78:7, 78:10, 123:16, 125:7, 125:14, 130:3, 139:15, 142:17, 143:1 allow 25:2, 58:19, 65:5, 72:18, 72:22, 92:18, 101:14, 122:3, 125:18, 135:15 allowed 100:2 almost 139:1 along 95:6, 97:19, 141:11 already 11:22, 109:22, 120:10, 121:4, 121:11, 122:6, 122:17 also 9:6, 10:17, 27:19, 30:1, 37:20, 73:18, 93:9, 96:11, 99:3, 99:12, 107:4, 108:12, 110:15, 120:4	alternative 143:6, 143:7 alternatively 107:19, 108:5 although 134:14 always 7:11, 117:1, 119:22, 120:3, 120:7, 121:1, 122:12, 137:4 amia 5:9 analysis 18:21, 33:7, 36:10, 40:16, 55:16, 55:22, 56:4, 56:9, 57:10, 66:2, 66:18, 67:1, 68:17, 88:11, 100:1, 100:11, 100:14, 100:22, 101:1, 114:19, 118:9, 118:16, 122:8, 126:7, 127:7 analytic 66:19 analytics 66:9 analyze 15:9, 55:21, 56:8, 56:10, 66:7 analyzed 40:17, 51:2 analyzer 55:4, 55:9, 55:19 analyzing 16:12, 55:11 anonymized 101:22 another 20:15, 28:4, 46:16, 58:8, 58:9, 58:12, 77:20, 104:4, 104:18, 136:7 answer 7:1, 7:7, 8:4, 37:6, 42:17, 42:19, 44:17, 68:18, 69:20, 71:13, 72:2, 84:16, 86:13, 117:12, 117:14, 117:15, 127:7, 130:11, 130:16, 132:21, 136:22, 137:2, 137:4, 137:6, 137:13, 137:15, 144:17 answering 136:21 any 6:13, 6:16, 7:11, 8:14, 12:19, 13:6, 14:7, 15:8, 19:9, 25:7, 26:6, 29:15, 30:19, 32:8, 42:9, 43:9, 46:20, 61:16, 65:4, 99:16, 99:17, 101:1, 103:2, 109:20, 110:10, 116:5, 117:7, 118:2, 118:9, 118:16, 123:20, 125:16, 139:6, 139:8, 139:13, 144:7, 146:17, 146:19 anybody 9:10 anyone 35:7, 55:22, 139:7, 144:8, 145:1 anything 9:2, 42:3, 42:6, 65:11, 100:12, 122:18, 130:12, 130:22, 142:8, 143:19 anyway 121:15 anywhere 32:13 apart 47:20 appeal 1:3 appear 33:4, 85:11 appearances 4:4 appearing 67:5 appears 93:16 append 45:12 applicant 108:17 application 4:21, 5:5, 18:14, 78:15, 78:16, 138:3 applied 40:15, 54:15, 98:21 apply 13:20, 28:15, 68:21 appreciated 79:9 approach 109:21, 136:15 appropriate 110:17, 110:20 approves 112:11 approximately 9:12 architect 13:13 architecting 33:19 architecture 32:5
--	---

architectures 28:20 area 68:9, 68:13, 100:19 areas 14:4 aren't 78:21, 79:1, 112:22 arise 20:9 arises 20:3, 20:5 arkansas 2:12, 2:17, 146:3, 147:10 around 9:14, 31:4, 55:2, 56:14, 59:15, 63:22, 72:12, 77:22, 79:6, 80:8, 83:13, 87:3, 91:15, 97:7, 115:21, 126:10, 127:11, 131:2, 133:1, 133:12, 140:4 arrivals 18:18 art 7:17, 7:22, 8:10, 8:22, 27:13, 27:17, 29:14, 29:18, 33:13, 62:16, 83:18, 128:6 asked 9:7, 63:14, 76:16, 108:7, 124:3, 127:6, 137:10, 139:22, 140:19, 141:22, 142:20 asking 7:15, 8:4, 14:16, 25:17,	27:12, 29:13, 71:21, 82:13, 116:13, 118:15, 123:2, 123:4 aspect 74:9 aspects 17:20 assertion 7:6 associate 36:5, 132:18 associated 40:9, 133:16 associates 132:17 assume 8:4, 14:3, 43:8, 50:10, 68:18, 69:20, 71:4, 78:9, 78:16, 84:10 assumes 123:22 assuming 16:8, 125:6 attach 106:16 attached 4:14, 5:2 attack 16:9, 42:11, 42:17, 42:20, 42:21, 43:1, 43:3, 43:8, 43:11, 44:14, 44:16, 46:14, 135:5, 135:9, 135:10, 135:13 attacked 15:20 attacker 43:6, 43:7, 46:14 attacks 43:19, 44:1, 44:4, 44:5, 44:7, 44:10,	44:12, 45:8, 46:4, 46:13 attempt 44:7, 135:10 attending 14:11 attorney 7:4, 146:19 attributes 51:3 audio 69:6 authentication 15:11, 28:21 authors 108:16 available 41:6, 66:1 avenue 3:5 aviel 1:15, 2:1, 4:6, 5:10, 6:2, 146:4, 146:14 avoid 99:12, 99:14 aware 20:19, 43:18, 45:6, 45:21, 46:2, 47:9, 130:13 away 109:2, 109:5, 109:7, 109:13, 109:15, 109:21	barclay 3:11 based 24:1, 98:3, 98:11, 126:18 basic 60:8 basically 21:10, 43:7, 70:14, 109:10, 121:5 basis 119:2, 119:3, 119:19 batch 15:18 because 14:4, 21:15, 23:5, 24:7, 31:15, 33:18, 35:12, 41:6, 44:5, 47:2, 47:5, 49:10, 57:6, 59:2, 66:22, 75:15, 76:18, 81:11, 85:21, 92:6, 95:20, 104:11, 119:18, 121:8, 122:16, 132:3 become 20:19, 43:18, 47:9, 58:10 been 9:12, 10:20, 11:4, 11:10, 11:16, 11:22, 18:5, 18:8, 18:9, 39:19, 44:20, 65:10, 66:1, 68:10, 72:7, 91:15, 99:6, 106:19, 110:1, 111:18, 115:10, 124:12, 124:22, 139:1, 140:13, 141:9, 143:11
--	--	--	---

before 1:3, 2:10, 7:2, 9:13, 16:5, 18:19, 31:10, 41:15, 41:19, 41:22, 42:3, 42:7, 52:5, 61:16, 100:9, 109:20, 134:3, 146:6, 146:8 began 144:6 begin 22:1 beginning 45:12, 93:16, 96:1, 137:20 begins 87:13, 136:15 behalf 3:2, 3:9 behave 52:22 behavior 66:10, 66:21 being 6:3, 12:12, 31:13, 31:20, 32:9, 33:20, 34:9, 45:7, 47:7, 57:13, 57:19, 57:20, 60:1, 69:2, 70:17, 71:1, 71:2, 83:1, 88:18, 88:19, 89:13, 98:19, 99:15, 108:18, 109:15, 117:4, 130:20, 135:8, 139:22, 140:19, 140:22, 141:22, 142:20 believe 27:10, 42:12, 42:14, 61:3, 91:16, 97:13, 101:6, 112:1,	118:2, 119:19, 127:16, 144:22 belong 122:6 belongs 123:8 below 126:13 benefit 90:10 beside 29:21 better 68:16 between 25:22, 26:2, 26:19, 27:1, 47:13, 57:18, 80:11, 82:3, 82:14, 82:17, 83:5, 96:17, 106:5, 112:13 bigger 44:2, 44:3 binder 8:17 birth 134:5 birthday 68:6, 73:2 birthdays 124:11 bit 17:17, 44:11 bits 44:13, 47:5, 47:7, 59:9 block 46:2, 46:7, 46:8, 46:10, 46:20, 47:4, 47:10, 97:21, 136:19, 136:20 blocks 46:11 blood 146:18 board 1:3	boss 46:21 both 19:20, 30:21, 50:14, 52:8, 54:9, 104:5, 104:22, 141:2 bottom 85:6, 106:1, 137:20 box 39:1 break 6:21, 7:2, 16:4, 33:21, 39:20, 39:21, 47:20, 69:18, 72:9, 87:2, 87:6, 115:12, 115:13, 139:2, 139:4, 139:16 breaks 6:20, 139:8 broad 78:20, 103:8 broader 100:1, 100:14, 106:8 broker 132:8, 132:13, 132:19 brought 54:7 bruce 97:18 build 22:17 bunch 48:20, 106:12, 121:6, 123:11 burden 130:6 business 17:21, 36:5, 132:17, 132:18 bypass 25:6 C california 2:14	call 13:11, 134:11 called 37:16, 45:6, 46:13, 92:16, 94:19 calls 94:19, 94:21 came 39:10, 126:3 camera 105:19 can't 8:18, 18:5, 36:10, 37:21, 47:4, 47:6, 59:13, 96:22, 111:22, 117:13, 122:8, 126:6, 128:1, 128:3, 130:16, 130:22, 134:19 candidates 97:14, 100:17 cannot 6:13, 36:19, 38:12, 65:11, 66:7, 86:5 capability 66:10, 66:20 capable 85:12, 85:19 capture 87:20 captured 88:5 care 92:20, 115:8 caregivers 91:19 carry 75:3, 142:5 case 7:11, 8:8, 33:10, 39:16, 48:5, 73:19, 77:12, 121:1, 121:12, 125:11,
---	--	--	---

125:13, 144:8, 144:19 cause 115:3 ccr 1:22, 147:8 central 94:11, 95:18, 104:9, 107:3, 131:6 centralized 39:9, 131:10, 131:14 centrally 104:5 certain 32:5, 32:6, 78:20, 79:1, 89:4, 89:11, 90:21, 101:9, 101:13, 107:5, 110:13, 111:6, 111:14, 111:15, 126:2, 136:1, 143:2 certificate 4:11, 146:1 certified 2:11, 146:2 certify 146:4, 146:10, 146:13, 146:17 chain 47:4, 47:10 chaining 46:2, 46:7, 46:10, 46:20 chair 17:15 change 135:1 changing 24:4 characterization 116:16 characterize 117:6 charge 104:18	checking 28:22 chooses 30:5 choosing 43:14 chose 9:5 chosen 42:15, 42:22, 43:2, 43:8, 43:22, 44:6, 44:12, 44:14, 97:17 citation 36:17, 85:7 citing 85:11 claim 30:13, 30:19, 31:3, 31:7, 31:12, 31:15, 31:18, 32:1, 32:6, 32:16, 32:19, 33:4, 33:9, 33:13 claims 128:22 clarification 135:2 clarify 7:13 clarity 10:11, 10:20, 11:4 clark 8:9 classic 46:17 clear 7:10, 34:16, 70:13, 107:11 clearinghouse 22:11, 22:15 client 138:2 clinical 47:18, 49:7,	49:15, 90:12, 90:20 clinically 96:5, 96:8 code 68:6, 73:3, 106:15, 137:12 coded 104:5 codes 68:10, 106:16 codified 106:2 codifying 106:6, 106:7, 106:8, 106:9, 106:11 collect 39:14, 93:2, 93:22 collected 94:3 column 31:3, 32:16, 50:19, 51:17, 53:18, 54:21, 55:1, 56:13, 57:15, 59:14, 60:3, 61:17, 62:10, 63:21, 66:3, 67:5, 72:12, 73:5, 73:6, 73:21, 74:19, 77:21, 79:5, 80:7, 82:9, 82:11, 82:12, 83:9, 83:22, 85:8, 115:18, 117:16, 117:20, 126:9, 127:11, 131:1, 132:5, 132:22, 133:11, 135:4, 135:18, 136:9, 136:13, 137:19, 138:11, 140:4, 140:18, 140:20, 141:19, 142:13	columns 140:2 combination 72:17 combinations 111:14 combine 20:13, 66:20 combined 120:17 come 49:21, 61:14, 89:1 coming 59:5, 70:22, 71:2, 99:9, 99:10 commencement 146:6 commencing 146:15 commission 147:4, 147:11 common 103:13, 103:17, 104:2, 104:8, 104:13, 104:21, 105:5, 105:10, 106:18, 140:9, 140:13 communicate 25:21, 59:13 communication 9:9, 91:4 communications 25:2, 25:7 companies 19:18, 26:15, 26:18, 26:20, 92:8, 102:10, 102:15, 102:21, 102:22 company 26:10, 47:15, 47:17, 47:22, 48:14, 49:5, 49:11, 102:9, 102:18, 103:1,
--	--	--	--

115:2 company's 48:5 compare 55:16 comparing 125:3 compatibility 58:6, 59:4 competently 53:1 competition 97:14 complete 57:10, 131:5 compliance 35:16, 36:8, 122:8, 126:6, 126:18, 127:14 compliant 34:4, 35:6, 36:12, 56:11, 68:1, 72:3, 94:7, 118:22, 119:11, 128:3, 128:12, 129:1, 129:3 complicated 58:10 complied 33:13 complies 128:20 comply 70:9, 127:21, 128:9 compromised 130:7 compromising 101:16, 101:20, 102:1 computer 9:3, 17:17, 76:1 concept 7:18, 19:10, 88:16 concepts 95:1	concern 84:19, 130:18 concerning 127:1 concluded 145:8 condition 49:17, 73:3, 104:12 conditions 49:12, 63:5, 91:13, 115:3, 124:12 conducted 1:14, 2:1 confidential 41:12, 53:3 confusing 53:9 connection 61:1, 105:5, 127:19 consider 24:18, 24:19, 29:19, 60:11, 139:13 considered 27:15, 27:20, 31:9, 34:20, 60:20, 61:9 consist 114:7 consistent 19:3, 31:20, 33:22, 61:1, 117:12 constitute 118:11 construction 40:8, 40:14, 40:15, 41:6 constructions 40:5 consult 110:16, 110:19 consulting-type 13:11 consumers 66:12	contain 62:3 contained 46:18, 90:4 contains 23:9, 46:22, 75:17 content 14:17, 14:19 contents 38:4 context 19:1, 30:16, 30:19, 31:16, 32:7, 35:3, 38:8, 47:12, 51:12, 52:2, 58:3, 62:15, 63:13, 75:12, 80:17, 84:14, 100:9, 117:9 contexts 141:16 contractual 30:7 contributed 13:1 control 26:9, 30:1 controlled 26:14, 26:17 controlling 25:14, 29:2 controls 26:3, 29:16, 30:1 conversations 139:6 coordination 26:22 copies 9:1 copy 8:17, 8:18, 103:19 core 17:17 correct 9:21, 10:4,	10:12, 10:21, 11:5, 11:11, 11:17, 12:1, 24:5, 31:5, 31:8, 31:14, 32:1, 33:1, 38:9, 39:3, 39:6, 39:11, 40:17, 48:3, 48:7, 48:12, 49:8, 49:13, 50:1, 51:7, 51:10, 51:15, 54:4, 54:7, 67:3, 67:11, 67:15, 68:22, 70:2, 70:19, 71:6, 71:9, 71:18, 77:15, 84:3, 92:4, 94:1, 94:13, 95:13, 95:21, 95:22, 103:5, 106:21, 107:6, 107:13, 114:5, 114:8, 120:1, 120:2, 120:5, 120:9, 120:13, 121:9, 122:14, 124:2, 127:14, 127:16, 128:16, 131:7, 131:16, 131:17, 131:21, 136:2, 136:11, 137:1, 142:6, 145:2 correctly 47:2, 142:18 correlate 125:9, 132:3 correlation 125:17 corresponding 40:5 corresponds 120:8, 121:7, 125:3 couldn't 15:8, 27:2,
---	---	--	---

120:16, 131:20 counsel 8:11, 8:12, 118:12, 140:1, 144:9, 144:10, 146:11 counterexample 123:14, 124:5 county 147:10 couple 17:11, 17:20 courses 17:7, 17:17, 17:19, 17:21, 19:8, 19:9 court 45:1 cover 10:1, 19:7 coverage 18:5 covered 18:9, 19:9, 36:2, 36:6, 69:22, 70:5, 70:6, 70:16, 70:18, 71:5, 129:20 covers 82:4 covid 68:9 crack 105:14 create 24:10, 24:13, 38:7, 54:9, 97:15, 98:11 created 34:18, 97:17, 99:1, 99:14 creates 24:14, 120:4 creating 14:18, 98:1, 129:9 creation 35:2, 130:3	criteria 101:9, 106:21, 107:1, 136:1 critical 100:17 cross-examination 142:1, 142:21 crunching 59:18, 60:3 cryptographer 97:18 cryptographic 14:21, 14:22, 15:3 cryptography 13:10, 13:20, 24:17, 37:15, 42:10 cst 1:17, 145:9, 146:16 curriculum 17:14, 18:4 cut 46:22 cut-and-paste 46:14 cypher 43:13, 45:20, 46:2, 46:7, 47:4, 47:10, 97:21 cyphers 44:10	104:5, 107:6, 134:1 databases 18:7, 18:13, 19:16, 19:19, 53:7 datasets 64:10 datavant 1:5 date 134:5 day 147:2 days 15:19 de-identification 21:18, 33:21, 42:8, 96:4, 109:20, 110:11, 111:11, 112:5, 112:14, 116:10, 118:22, 119:4, 122:12, 124:14, 125:8, 127:4, 127:12, 128:15, 128:22, 129:3, 129:13, 131:5 de-identified 21:17, 22:14, 38:22, 39:5, 65:8, 65:10, 68:10, 93:17, 101:22, 110:1, 118:5, 119:7, 119:14, 120:4, 120:8, 120:11, 120:19, 121:6, 122:13, 122:22, 123:6, 123:8, 123:11, 123:16, 124:1, 124:22, 125:2, 125:10, 125:15, 126:1, 131:11, 133:15, 134:3, 141:12 de-identifies 111:2	de-identify 70:12, 95:5, 110:18, 111:4, 119:10, 119:13, 129:8 de-identifying 110:9, 110:22, 111:8, 111:19, 112:12, 113:10, 113:12, 113:14, 126:15 deal 15:12 dealing 116:22 dealt 17:19 death 115:4 decide 13:2 decides 29:3 declaration 5:10, 8:8, 8:19, 9:21, 12:4, 12:7, 12:10, 14:13, 16:18, 21:1, 22:19, 30:17, 30:18, 32:11, 32:13, 33:11, 34:6, 36:14, 37:8, 38:14, 40:2, 80:22, 85:4, 86:20, 103:10, 105:1, 108:21, 112:2, 112:17, 118:18, 128:14 declarations 8:9 decrypt 34:20, 45:18, 47:2, 47:7, 76:11, 76:12 decrypted 16:10
	D		
	database 18:19, 20:20, 22:9, 39:2, 39:5, 42:2, 50:15, 53:11, 53:12, 58:3, 58:19, 60:7, 62:9, 62:19, 63:1, 70:1, 70:15, 70:16, 71:9, 71:16, 88:20, 94:11,		

decrypting 85:13, 85:20 decryption 35:1, 52:8, 74:5, 74:14, 74:18, 77:14, 77:19, 77:20 define 37:19 defined 60:6, 94:9 definitely 20:4, 84:22 definition 51:1, 111:11, 112:14 delete 15:14, 16:3, 16:14 deleted 123:1 deleting 15:8 departments 13:15 depend 28:19, 41:4, 54:12, 54:13, 78:14, 138:9 dependent 138:1 depending 123:10 depends 41:3, 49:14, 119:16 deployed 34:3 deposed 9:13 deposes 6:3 deposition 1:14, 2:1, 7:5, 8:6, 8:7, 9:10, 61:10, 146:5, 146:7, 146:12, 146:13	depositions 9:15 depression 136:11, 137:11 derived 99:6 derives 31:8 describe 23:1, 28:12, 29:12, 44:18, 131:22, 141:3 described 16:13, 29:9, 29:20, 30:17, 33:5, 38:11, 57:13, 64:21, 80:19, 89:13, 101:6, 107:14, 108:12, 111:5, 112:19, 117:8, 118:3, 118:11, 127:21, 128:8, 134:17, 138:20 describes 25:19, 31:17, 32:5, 67:10, 81:9, 91:9, 94:6, 95:3, 110:13, 129:7, 137:8 describing 93:17 description 4:15, 5:3, 28:8, 31:21, 98:16, 118:6, 135:19 design 32:1, 112:4 designed 15:6, 135:11 designer 88:7 designing 15:11, 128:12 designs 111:20, 111:21	desirable 90:11 destination 76:2, 76:4, 76:6, 76:8 destroy 121:13, 121:17 destroyed 41:14, 119:13 destroying 121:18 detail 31:1, 76:15, 88:4 details 64:19 detect 20:16 determine 47:16, 48:2 determining 115:6 device 103:2, 103:5 devised 25:5 diabetes 100:19 diagnosis 136:10 dick 5:6, 11:8, 110:2, 113:7, 113:21, 114:2, 114:10, 114:13 difference 47:13, 82:2, 82:14, 82:17, 83:4, 99:16, 106:5, 112:13 different 13:15, 15:5, 17:11, 19:3, 19:16, 19:22, 26:14, 26:17, 29:9, 37:19, 39:15, 39:16, 43:19, 45:8,	45:17, 46:3, 46:12, 49:7, 52:11, 56:3, 57:2, 59:5, 59:11, 60:12, 63:10, 63:18, 68:4, 70:14, 70:22, 71:2, 71:4, 75:9, 77:14, 79:18, 79:19, 79:20, 79:21, 87:21, 89:12, 91:10, 91:12, 91:19, 92:7, 92:8, 92:13, 94:4, 99:18, 100:15, 104:19, 106:13, 106:16, 109:12, 112:22, 113:4, 113:16, 113:19, 115:6, 123:12, 124:11, 124:12, 124:13, 125:4, 128:5, 129:7, 138:7, 141:15, 141:16 digest 121:16 digestible 47:21 direct 118:13 direction 80:10, 109:12 director 17:7 disagree 116:5, 128:18 discard 15:1 discarded 54:19 disclose 142:8 disclosed 143:6 discloses 107:9, 109:6,
---	--	--	--

109:8 disclosure 128:18, 140:20, 142:1, 142:21, 143:1 discuss 8:11, 32:12 discussed 49:21, 54:4, 60:1, 60:2, 77:17, 105:2, 109:15, 127:11, 138:13, 144:15 discusses 114:4 discussing 66:17, 106:20 discussion 54:7, 56:14, 59:17, 96:15, 98:1, 105:5, 110:8, 117:19, 133:14, 134:15, 136:18, 140:1, 144:14 discussions 144:7 disease 62:21, 63:2, 68:13 disseminated 68:19, 68:22, 69:21, 130:14 disseminating 29:5, 29:17, 30:4 dissertation 14:20, 15:13 distinction 48:18 distributable 116:1, 116:9 districts 20:12, 20:13 doctor 13:17, 65:15, 120:10, 120:13, 121:1, 122:16,	124:3, 124:13, 124:21, 125:2, 125:9, 125:14, 125:18, 125:22, 130:13, 130:19 doctor's 119:9, 119:12, 119:22, 120:3, 120:7, 121:12, 121:14, 121:22, 122:1, 122:2, 122:5, 122:11, 123:5, 124:10, 124:15, 129:21, 129:22, 130:5 doctors 13:8, 14:12, 71:4 document 130:17 documents 9:5, 9:8 doing 28:7, 28:9, 32:3, 32:4, 61:13, 61:15, 72:4, 108:15, 129:20, 137:3, 137:9 domain 17:18 domains 20:4, 20:9 done 94:7, 138:8 down 18:19, 61:14, 89:17, 97:7, 107:18, 121:17 download 9:7 dozens 103:2 dr 6:8, 40:1, 72:11, 87:8, 115:15, 118:13, 139:6, 144:5,	144:16 draw 48:18 drug 64:17 duly 6:3, 146:6 during 7:5, 9:10, 80:2, 139:8, 142:1, 142:21 E e-mail 9:10 each 25:21, 49:20, 57:22, 119:8, 124:10, 140:8 earlier 13:4, 54:4, 54:7, 56:13, 106:14, 108:12, 129:12, 132:14 early 25:1, 115:4 ease 7:20, 45:1 easier 44:15 educational 16:21 either 30:7, 42:21, 50:9 ekenseair 1:22, 2:11, 146:2, 147:8 elected 75:2, 142:4 electronic 88:11, 89:6 elements 107:5, 133:15, 138:15 else 22:6, 70:8, 81:21, 99:10,	123:19 embodiment 31:18, 33:5, 33:8, 80:19, 82:15, 82:18, 83:1, 102:7 embodiments 78:3, 80:9, 82:2, 82:3, 82:7, 82:15, 83:2, 89:4, 89:11, 101:14, 118:10, 118:13, 142:16, 143:3 employed 146:19 employee 46:19 encoded 94:20 encompass 82:19, 100:14, 106:9 encompassed 88:16, 113:12 encrypt 16:2, 24:13, 41:8, 45:15, 57:7, 74:16, 76:5, 77:4, 79:3, 80:2, 140:8, 140:17 encrypted 25:3, 41:9, 46:15, 46:19, 46:21, 47:3, 77:5, 78:4, 78:10, 78:11, 78:21, 79:1, 80:5, 129:9, 133:4, 133:5, 133:16, 141:11, 142:17, 143:2, 143:8, 143:13 encrypting 38:7, 41:1, 78:7, 79:19, 129:11, 141:3,
---	--	---	---

143:10 encryption 23:5, 23:15, 23:16, 23:17, 23:19, 23:22, 25:11, 25:14, 26:5, 27:2, 27:5, 27:7, 27:21, 28:2, 28:9, 28:16, 29:3, 29:16, 30:8, 31:13, 31:19, 32:9, 34:19, 35:18, 36:3, 36:7, 37:1, 41:5, 43:10, 44:19, 45:14, 45:16, 46:8, 46:10, 47:6, 52:7, 54:6, 54:15, 56:15, 74:5, 74:14, 74:17, 75:2, 75:4, 75:8, 75:9, 75:20, 76:13, 76:16, 76:22, 77:2, 77:3, 77:7, 77:9, 77:17, 79:10, 79:16, 84:2, 84:6, 84:9, 84:15, 97:15, 122:2, 124:15, 124:17, 140:9, 140:13, 140:16, 142:4, 142:6, 143:20 end 19:22, 22:19, 75:16, 75:21, 95:2, 97:22, 105:22, 144:5 endeavor 6:20 ended 15:11 endusers 102:8	english 56:6 enhanced 76:13 enough 44:9, 50:13, 58:14, 66:22, 75:15, 132:21 ensure 19:21 ensures 86:5 ensuring 19:1, 61:1, 91:19 entered 107:20 entire 79:3 entities 19:4, 25:14, 71:6, 109:19, 122:11 entity 25:14, 29:16, 29:22, 30:3, 30:4, 36:2, 36:6, 57:22, 69:22, 70:16, 70:18, 71:18, 80:4, 80:12, 80:20, 129:19, 129:20, 130:15 entry 60:7, 62:9 environment 15:16, 15:17 epid 95:4, 95:8, 95:13, 95:17, 97:1, 97:5, 97:6, 98:11, 99:1, 99:11, 99:13, 99:18 epids 94:21, 96:15, 98:2, 101:5 equivalent 81:22	escrow 23:21, 24:16, 24:19, 24:21, 51:21, 52:3, 52:4, 52:7, 52:10, 52:14 escrowed 25:9 esquire 3:3, 3:10, 3:11 essentially 136:18 established 86:6 establishing 119:6 etcetera 59:20, 68:7 even 24:7, 44:9, 51:5, 117:2 evenhaim 4:19, 10:17, 50:16, 51:17, 53:19, 54:21, 57:6, 57:15, 58:22, 59:3, 59:14, 61:17, 62:10, 63:21, 66:3, 66:6, 67:10, 67:13, 67:16, 72:11, 73:21, 74:19, 76:14, 77:21, 78:17, 79:5, 80:7, 81:4, 81:8, 82:1, 82:6, 82:9, 83:9, 83:22, 84:10, 85:7, 86:1, 109:14, 109:18, 139:19, 140:2, 140:22, 141:9, 143:9, 143:17 evenhaim's 84:7, 140:1 ever 70:11	every 6:20, 45:14, 123:22 everybody 100:18, 106:17 everyone 105:10 everything 9:1, 59:8, 123:19 exact 131:8 exactly 95:14 examination 4:7, 4:8, 4:9, 6:6, 139:17, 144:3 example 15:17, 18:15, 19:17, 20:11, 21:14, 22:7, 22:10, 24:16, 24:22, 27:1, 31:18, 33:5, 34:17, 35:21, 44:11, 46:17, 48:9, 50:7, 55:18, 59:8, 59:19, 62:20, 63:7, 64:21, 65:9, 68:4, 76:5, 77:11, 77:16, 80:2, 81:16, 90:2, 90:22, 91:11, 96:10, 98:2, 100:18, 102:17, 102:20, 103:22, 104:3, 104:12, 104:20, 106:12, 115:1, 115:9, 117:10, 120:17, 124:7, 125:5, 125:18, 131:15, 133:9, 135:13, 135:22, 136:4, 136:7, 136:9,
---	--	---	--

137:9 examples 54:16, 73:11, 76:21, 89:12, 92:13, 102:21, 111:3, 118:13, 138:21, 143:14, 143:17 exclude 83:19 excluding 83:20 exclusively 46:9 excuse 45:7, 102:6 exemplary 102:7 exhaustive 44:8, 44:16 exhibit 4:16, 4:18, 4:20, 5:4, 5:7, 5:9, 5:10, 9:18, 10:4, 10:6, 10:7, 10:21, 11:1, 11:5, 11:7, 11:10, 11:13, 11:16, 11:19, 12:1, 12:3, 50:17, 87:9, 110:3, 115:16, 134:9 exhibits 4:13, 5:1, 8:19, 8:20 existing 66:9, 66:19, 67:11 exists 35:18 expect 26:18, 65:17 expecting 27:3 experience 41:15, 41:18, 41:21, 42:7,	110:17, 110:20, 112:11 expert 9:16, 112:10 expires 147:4 explain 19:13, 21:8, 30:22, 35:12, 37:13, 43:5, 46:6, 82:2, 94:22, 97:11, 134:16 explained 126:13 explains 142:3 explanation 121:20 extending 117:20 extends 12:9 extent 134:6 F facilitate 93:6 facilitated 79:12, 79:17 facilities 19:21 fact 38:12, 57:7, 59:1, 62:6 fair 7:2, 65:6, 75:10, 81:15, 85:14, 86:1, 94:8, 114:11, 115:8 familiar 7:18, 19:6, 19:10, 19:12, 42:11, 42:20, 43:2 far 93:9, 97:19,	134:20 farther 97:7 fashion 57:1 features 51:3 feedback 14:11 female 136:5 few 72:17, 144:7 field 13:20, 18:12, 24:17, 34:1, 42:4, 42:10, 43:22, 47:1, 53:14, 58:14, 62:7, 132:12, 134:3, 134:4, 134:5 fields 59:11, 59:12, 68:5, 68:20, 72:17, 72:22, 78:21, 111:6, 112:21, 113:5, 114:17 figure 22:19, 22:20, 23:2, 23:20, 25:13, 27:4, 31:18, 32:1, 33:6, 39:1, 39:7, 121:7, 123:7, 125:2, 135:18 file 38:3, 38:4, 46:18, 46:21, 47:1, 145:7 files 71:8, 107:3 final 145:3 finalists 97:17	financially 146:21 find 15:8, 16:6, 37:21, 38:12 finding 136:9 fine 6:10 fingerprint 18:21 fingerprinting 18:16 firewalls 28:21 first 6:3, 20:19, 34:8, 43:18, 45:21, 47:9, 55:1, 64:2, 79:8, 83:12, 88:10, 96:15, 99:22, 101:13, 113:9, 141:1 fish 3:12 fit 15:10, 58:13, 58:14 five 105:22, 123:15, 124:9 five-minute 39:20 fixed 37:17 flexibility 108:17, 108:18 fly 122:9, 126:7 focus 12:11, 12:18, 13:3, 17:18 focused 16:21 folder 9:6 follow 40:22, 90:20
--	--	---	--

follows 6:5 footnote 21:5, 21:8, 21:10, 22:3, 23:1, 30:17 form 19:5, 22:2, 23:7, 27:18, 32:2, 35:10, 56:5, 64:7, 69:5, 70:2, 70:3, 70:20, 71:17, 71:20, 82:5, 82:20, 107:7, 116:17, 116:21, 122:7, 129:9 format 57:20, 58:5, 58:19, 59:1, 59:6, 59:7, 59:13 formats 61:1 forming 61:6 formulate 16:11 forth 91:7, 124:19, 146:6 found 81:2, 87:15 founded 17:6 four 14:8, 56:14, 89:17, 123:17 frame 47:11 freely 115:22, 116:8 friday 1:16 front 8:14, 9:21, 10:7	full 62:19, 68:15, 90:10, 104:15, 130:2, 138:12 fully 77:12, 90:18 function 24:8, 37:10, 37:13, 37:14, 38:6, 38:11, 38:13, 45:16, 54:11, 97:5, 98:21 functionality 25:20, 32:6 fundamental 80:11 funding 13:2 further 4:9, 80:1, 87:13, 87:19, 127:7, 139:11, 144:2, 144:3, 144:20, 146:10, 146:13, 146:17 furthermore 80:9 fuzzy 60:4	generally 52:9, 83:3, 88:11 generate 21:15, 23:12, 36:20 generation 30:22 generator 27:22, 29:6, 29:17, 30:4 geography 51:2 georgia 2:13 getting 6:11, 48:10 give 6:13, 6:17, 24:21, 34:17, 106:14, 119:3, 137:2 given 14:7, 38:13, 59:19, 61:15, 64:8, 64:9, 138:21, 146:9 gives 98:3, 110:14 giving 50:7, 137:4 go 22:14, 61:12, 69:15, 72:8, 87:3, 92:20, 96:22, 113:22, 115:11, 116:18, 123:21, 125:19, 127:2, 139:3 goal 58:16, 60:19, 61:3, 67:13, 81:9 goes 74:8, 76:14, 88:22, 141:3 going 13:1, 13:7, 25:16, 36:18, 39:19, 48:19, 48:20, 48:22, 49:1, 58:19, 63:12, 72:7, 80:17, 81:20, 83:22, 86:22, 103:19, 115:1, 115:10, 118:17, 127:2, 138:9, 139:1 good 6:8, 6:10, 7:3, 49:19, 87:5, 90:20, 132:2 government 25:2, 25:4 grant 13:2 granularity 87:21, 88:6 great 12:4 group 47:16, 48:10, 48:11, 48:15, 48:20, 49:1, 65:3, 66:11, 66:21, 100:21, 114:8 growth 90:11, 90:18 guard 27:17, 44:3, 45:7 guarded 43:22 guess 19:11, 42:17, 103:8, 105:22, 111:7, 116:15 guys 69:7, 69:11
	G gain 13:19 gave 81:16, 125:6, 125:14 general 14:18, 50:6, 52:12, 75:2, 77:1, 84:19, 84:21, 85:2, 86:2, 86:11, 107:9, 113:4, 124:3, 124:6, 142:4 generalized 16:13	H half 94:18 hand 147:1

handled 54:14, 54:17 hands 43:15 happen 23:2, 68:14 happened 92:6 happening 28:13 happens 59:3, 109:19 happy 33:11 harbor 103:1 hardware 28:19 hash 37:9, 37:13, 37:14, 37:20, 38:3, 38:6, 38:10, 38:11, 38:13, 53:22, 54:3, 54:11 hashed 24:8 head 71:14, 112:1, 117:14, 130:5 heading 81:4 health 17:22, 48:1, 48:15, 66:12, 114:18, 124:2, 125:6, 125:15, 126:2, 126:17 healthcare 12:12, 12:17, 12:20, 16:22, 17:12, 17:18, 19:18, 21:11, 31:5, 32:20, 33:2, 47:12, 49:22, 57:10, 62:15, 63:5, 65:2, 66:9,	66:19, 68:16, 84:12, 86:3, 86:7, 104:16, 104:18, 116:9, 126:17, 129:7, 130:1, 141:2 hear 47:19, 69:7, 69:8, 69:10, 69:14, 70:21, 85:16 height 62:22 held 25:8, 35:7, 51:21, 97:14, 124:9 hello 69:13 helpful 31:1, 57:4, 104:21 here 8:18, 36:10, 37:5, 38:22, 39:8, 48:18, 57:14, 60:14, 65:9, 67:6, 84:8, 89:13, 98:20, 101:6, 103:18, 105:16, 106:20, 107:14, 111:5, 117:15, 135:8, 135:13, 136:4, 138:20, 140:22, 141:10, 143:6 here's 123:14 hereby 146:4 hereinbefore 146:5 hereunto 147:1 high 67:2, 67:17, 70:2, 70:19,	81:12, 81:17 high-level 59:9 high-resolution 67:7, 67:21, 71:17 highest 81:19 highly 90:11 hipaa 16:22, 33:14, 33:22, 34:4, 35:6, 35:14, 35:17, 35:19, 35:21, 35:22, 36:2, 36:8, 36:12, 68:4, 68:21, 70:6, 70:9, 71:3, 71:11, 71:22, 72:3, 84:18, 86:11, 86:15, 94:7, 94:10, 116:2, 116:6, 116:11, 116:14, 116:19, 117:1, 117:6, 117:7, 117:10, 117:12, 118:2, 118:4, 118:7, 118:11, 119:1, 119:11, 119:15, 121:17, 121:19, 122:4, 122:8, 126:5, 126:6, 126:19, 127:1, 127:5, 127:14, 127:22, 128:9, 128:13, 128:16, 128:20, 129:1, 129:3, 129:12, 129:20, 130:4, 130:8, 130:12, 130:17, 132:16, 132:20 hipaa-compliant 37:2 hl7 91:2, 91:3,	91:15, 92:7 hold 52:5, 52:7, 86:22 holding 25:10, 52:11 holds 34:19, 124:16 hopkins 12:22, 13:5, 13:15 hospital 71:5 hostile 15:16, 15:17 hot 105:16 hour 6:21, 39:20, 72:8, 115:11, 139:2 housekeeping 6:12 hr 46:19, 47:1 human 114:7 humans 114:8 hypothetical 28:4, 29:8, 30:6, 36:11, 123:22, 124:18 I icu 13:16 id 40:20, 51:5, 56:15, 73:8, 133:4 idea 58:7, 60:8, 85:12, 99:1, 100:10, 105:7, 111:14 identical 81:21
--	--	---	---

identifiable 21:13 identification 9:18, 10:6, 11:1, 11:7, 11:13, 11:19, 12:3, 65:5, 72:18, 73:1, 79:11, 79:17, 85:20, 114:5, 119:11 identified 21:11, 61:7 identifier 40:9 identifiers 94:19, 94:20 identify 33:2, 57:9, 86:9, 86:17, 89:6, 95:3, 100:21, 119:20, 120:8, 120:18, 129:11, 141:4 identifying 19:2, 21:18, 24:4, 30:21, 40:21, 64:18, 94:13, 95:12, 95:15, 100:16, 110:14, 111:8, 112:15, 123:18, 133:5, 140:8 identities 34:9 identity 40:10, 41:7, 55:3, 62:4, 72:15, 86:5, 102:2 identity-free 61:21, 62:2 ids 73:11, 73:14, 133:17 illinois 2:13 illustrated 31:17	image 37:16 imagine 49:16 impersonate 27:8 implement 33:13 implemented 126:16 implications 82:22 importance 58:4 important 85:18 inc 1:5 include 24:9, 49:4, 51:1, 51:5, 51:10, 51:14, 53:2, 74:4, 78:17, 83:14, 83:18, 93:10, 96:11, 102:8 includes 21:5, 24:12, 72:15, 79:3, 86:7, 114:5 including 72:16, 75:3, 142:5 inclusion 73:7 increasing 15:4 independent 92:17, 93:1 indicate 128:7, 143:19 indicates 64:16, 75:1, 79:9, 96:16, 127:19 indicating 51:9 indicative 99:2, 99:5	individual 40:10, 40:11, 40:21, 41:7, 57:12, 65:11, 65:12, 75:3, 75:17, 79:11, 79:16, 86:18, 95:4, 101:1, 114:8, 119:21 individual's 85:22 individuals 24:2, 34:9, 49:11, 49:16, 51:5, 51:14, 73:8, 73:12, 79:12, 84:11, 100:13, 142:5, 142:9, 143:21 industries 44:22 industry 44:21 infarc 104:6 infarction 104:4, 104:13 informatics 13:18 information 15:2, 15:5, 16:7, 16:15, 19:1, 19:2, 21:12, 21:14, 22:14, 23:6, 23:7, 23:13, 23:18, 24:4, 26:6, 26:7, 26:13, 28:16, 30:10, 30:21, 31:5, 32:20, 33:3, 36:12, 39:14, 40:21, 46:19, 49:18, 49:21, 50:13, 51:14, 53:3, 54:15, 56:3, 56:8, 58:16,	58:18, 59:5, 65:2, 65:17, 67:22, 75:18, 77:13, 84:17, 85:13, 85:20, 86:8, 86:17, 87:14, 87:20, 88:4, 89:18, 89:22, 90:1, 90:3, 90:4, 90:12, 90:20, 93:18, 94:13, 95:5, 95:12, 95:16, 96:5, 96:9, 100:1, 100:10, 101:14, 101:18, 101:19, 101:21, 102:20, 110:14, 111:8, 111:11, 111:15, 112:8, 112:15, 112:19, 113:1, 113:5, 114:19, 117:1, 119:12, 119:20, 120:16, 120:17, 123:19, 124:2, 125:7, 125:15, 126:2, 132:4, 133:6, 134:2, 135:11, 135:15, 141:11 infusible 37:19 infusion 102:18 initiating 27:6 input 37:16, 38:2, 46:9, 48:20, 49:17 insights 130:3 instance 18:3, 23:17, 25:10, 26:3, 26:10, 47:15, 49:12, 56:2,
--	---	--	---

64:16, 69:22, 95:11, 95:19, 98:12, 104:16 instances 9:15 instant 51:4, 78:3, 80:10, 142:16 institute 45:4 institutions 91:10, 91:12 instructions 16:2 insurance 47:15, 47:16, 47:22, 48:5, 48:14, 114:17, 115:2, 115:7, 115:8 insuring 48:2 integrity 47:8 intend 7:20 intended 127:21, 128:9 intention 127:19, 128:2 intentions 128:4 interest 13:19 interested 13:17, 14:10, 81:16, 101:15, 131:19, 143:9, 146:21 interim 15:21 introduced 92:7 introduction 134:12 invention 28:2, 28:11, 34:1, 79:2,	88:10, 89:1, 102:8, 126:14, 127:20 inventors 128:1, 128:11 investigator 14:9 involve 60:4, 143:21 involved 14:7, 14:15, 14:18, 15:7, 121:18, 122:9 involves 67:18 ipr 1:11, 10:2 ipsec 74:16 irreversibility 36:1 irreversible 36:15 issue 15:15, 16:11, 19:7, 20:20, 49:22, 58:6 issued 64:18, 64:20 issues 75:16, 75:21, 116:2, 116:6, 116:11, 116:14, 116:20, 117:2, 117:6 items 59:18, 60:14, 99:17 itself 52:21	16:5, 16:7, 16:8, 16:10 jobs 15:15, 15:16 johns 12:21, 13:4 joined 17:6 joining 60:14 joins 60:16 judgments 36:11 justin 3:3	140:9, 140:13, 140:16, 140:17, 141:9, 141:14 keys 25:3, 25:6, 25:7, 25:11, 44:2, 44:3, 44:11, 52:5, 52:7, 52:12, 56:19, 57:1, 57:4, 57:8, 57:11, 115:22, 116:8, 117:3, 140:1, 141:2, 141:4 kind 23:10, 92:11, 119:7, 135:1 know 6:21, 7:13, 13:11, 19:8, 21:22, 27:16, 28:3, 28:20, 36:8, 49:11, 53:9, 61:12, 63:1, 68:6, 68:12, 75:19, 82:21, 86:22, 87:14, 91:16, 92:11, 93:7, 100:18, 105:12, 107:8, 115:3, 118:1, 120:11, 121:16, 123:7, 123:14, 125:18, 130:8, 130:9, 130:10 knowable 55:4, 55:9 knowing 55:13 knowledge 13:8, 13:9, 110:17, 110:20, 112:11 known 28:15, 34:2, 42:12, 42:15,
	J	K	
	jacket 105:15 jeffrey 3:11 job 1:20, 16:1,	karisa 1:22, 2:10, 146:2, 147:8 keep 26:7, 33:20, 120:20 kept 41:11 kerberos 15:7 key 15:8, 15:14, 16:2, 16:3, 16:7, 16:10, 16:15, 24:3, 24:7, 34:19, 35:1, 35:7, 35:18, 36:3, 36:6, 41:5, 41:9, 41:11, 44:7, 44:9, 44:14, 47:3, 51:20, 54:14, 54:17, 54:19, 57:7, 117:4, 119:13, 121:13, 121:17, 121:19, 122:2, 122:3, 124:16, 129:19, 130:6, 130:14,	

42:20, 42:21, 43:11, 43:22, 44:6, 111:18, 113:17, 132:16 knows 49:11, 122:6	leading 141:18, 142:11, 143:4, 143:22 leaking 28:17 least 26:21, 101:22, 120:13, 128:19 left 59:9, 123:17 legal 17:20, 82:13, 82:22 length 37:18 lengths 117:4 less 111:12, 137:7, 137:13, 137:15 let's 12:4, 14:1, 16:5, 18:15, 19:17, 38:2, 45:13, 46:17, 62:20, 68:7, 71:4, 72:8, 78:16, 84:10, 102:17, 120:20, 122:1 level 62:19, 63:4, 64:11, 64:13, 64:14, 65:9, 65:18, 68:11, 75:2, 75:4, 76:15, 81:10, 84:2, 88:6, 142:4, 142:6 levels 76:21, 87:21 life 45:1, 114:18, 115:2, 115:7 likely 75:9, 93:5, 120:6 limit 31:7, 138:14	limitation 31:11, 66:17 limitations 102:22 limited 103:4 limiting 33:8, 138:22 line 31:3, 32:17, 37:9, 38:17, 50:20, 51:18, 53:18, 56:14, 57:16, 59:15, 60:3, 61:18, 62:11, 63:22, 64:2, 66:4, 67:5, 72:12, 73:6, 73:22, 77:22, 79:6, 80:8, 82:10, 83:10, 83:13, 115:19, 115:21, 117:17, 117:20, 126:10, 127:11, 131:2, 132:5, 133:1, 133:12 lines 55:2, 57:18, 74:2, 74:20, 83:22, 85:8, 89:17, 106:1, 107:18, 140:5, 140:20, 141:21, 142:15 link 57:9, 63:9, 63:10, 63:17, 63:18 list 40:4, 50:22, 51:4, 60:6, 66:11, 66:22, 68:20, 72:16, 73:7, 75:3, 75:8, 78:4, 78:8, 78:17, 78:18, 79:4,	84:2, 84:6, 84:11, 110:14, 114:11, 129:11, 142:5, 142:10, 142:17, 143:2, 143:8, 143:10, 143:20 listed 112:8 lists 68:4 literal 53:8 literature 15:4 little 6:11, 9:19, 36:11, 47:20, 60:2, 135:19 llc 1:8 llp 3:4 located 81:18 location 20:18, 106:22 locations 79:10, 79:16 logic 15:11, 60:4, 138:14 logically 91:22 long 26:11, 58:14, 71:17, 91:15, 106:14 long-running 15:15 long-term 115:8 longer 66:8, 113:5 longitudinally 61:7 look 16:17, 27:1,
L			
labs 103:1 landi 5:8, 11:14, 115:15, 115:18, 116:16, 117:16, 118:11, 118:16, 126:9, 126:22, 127:10, 128:8, 128:19, 128:21, 129:7, 131:1, 131:22, 132:5, 132:8, 132:22, 133:11 landi's 127:4, 127:19, 128:15 language 56:7, 78:19, 80:16, 103:6 large 17:22, 44:9, 62:9 last 30:13, 37:9, 55:2, 69:4, 86:13, 90:9, 98:7, 109:1, 135:4, 138:12 later 33:10, 73:5 latest 12:11, 12:15 launch 44:5 lawful 6:3 lawyer 82:21 lawyers 17:20			

36:4, 36:17, 36:18, 38:14, 48:8, 50:7, 59:14, 62:10, 63:1, 65:12, 71:13, 72:5, 74:19, 82:9, 83:9, 91:2, 94:15, 101:4, 101:12, 113:7, 114:13, 117:13, 117:16, 128:21, 132:20, 132:22, 134:12, 137:17, 138:11, 140:4, 141:19 looked 88:19, 91:8, 92:3 looking 10:1, 18:17, 27:4, 31:3, 31:10, 32:16, 47:15, 47:17, 48:14, 49:5, 52:13, 62:7, 62:9, 88:9, 95:2, 96:14, 101:8, 130:16, 131:19, 136:13 lost 66:1, 69:6 lot 9:7, 13:8, 13:9, 13:19, 44:15, 121:18 lots 72:15 low-resolution 66:18 lower 65:19, 65:21, 66:8, 67:8 ls 147:8 lunch 87:3 M machine 16:4, 16:5	made 9:2, 97:18 maintain 67:21, 70:1 maintained 70:18, 71:16, 96:17 maintaining 53:2, 126:18, 127:14 make 13:2, 36:10, 44:15, 47:20, 88:8, 102:10, 102:15, 103:6, 111:1, 113:4, 134:1 makes 21:20, 93:12, 102:18, 104:10, 122:20 making 26:12, 112:10, 119:19, 130:7, 135:1 management 17:12 managing 17:21 manic 136:11, 137:11 manner 38:6, 94:7, 109:14, 112:18 manufacturers 103:2, 103:5 many 8:12, 9:12, 13:22, 14:2, 20:3, 44:21, 114:17, 138:7 map 99:11 mapping 96:17 mappings 97:6 marked 9:18, 10:4,	10:6, 10:20, 11:1, 11:4, 11:7, 11:10, 11:13, 11:16, 11:19, 11:22, 12:3 marks 9:2 marriage 146:18 massachusetts 3:5 masters 17:5 match 21:16, 109:22, 125:16, 135:15 matched 23:8, 129:18, 130:1 matches 125:16 matching 41:22, 42:1, 60:4, 109:19, 120:9, 122:13, 136:1 materials 8:8 matter 26:11, 81:18, 129:21, 146:22 maybe 14:8, 20:13, 20:16, 35:12, 53:12, 62:7, 91:2 mean 14:3, 18:10, 18:18, 19:13, 34:13, 38:1, 38:20, 39:13, 55:15, 59:7, 62:5, 64:15, 68:3, 70:8, 70:10, 76:8, 78:20, 79:15, 80:16, 81:7,	96:21, 102:16, 103:1, 105:8, 108:2, 108:4, 109:8, 124:5, 138:6 meaning 53:11, 76:10, 79:21, 80:10, 103:17, 105:4 meanings 141:15 means 29:19, 29:22, 30:2, 36:18, 39:14, 48:10, 55:10, 56:8, 65:22, 78:9, 81:11, 88:3, 96:22, 102:6 meant 21:8, 36:16, 65:21, 66:15, 76:17, 78:7, 79:2, 88:2, 138:18 mechanism 16:12, 24:3, 24:10, 24:12, 24:15, 30:19, 30:22, 34:19, 110:22 mechanisms 91:19 medical 13:7, 13:15, 13:18, 13:21, 14:3, 14:6, 14:10, 19:19, 20:4, 20:5, 22:14, 23:6, 23:7, 23:12, 42:2, 42:4, 50:8, 53:6, 53:14, 86:16, 88:12, 88:17, 88:20, 89:6, 90:4, 90:10, 90:19, 91:1,
---	---	--	---

91:4, 91:9, 92:8, 92:10, 92:14, 101:4, 102:10, 102:15, 102:19, 103:2, 103:6, 103:7, 111:19, 113:15, 114:18, 117:1, 124:12, 130:19, 130:20, 132:4, 135:14 medication 6:16, 56:12 medications 96:10, 124:13 meet 8:12, 101:9, 119:4, 119:5, 119:6 meeting 8:10, 13:7 members 102:9 memorized 130:9 memory 59:10 mention 76:3 mentioned 9:20, 127:3, 129:12 merged 19:18, 20:2 merger 79:11 merging 19:16, 80:4 merit 2:15 message 26:22, 27:6, 46:15, 46:16, 47:6 method 78:12, 111:1, 118:22, 124:15, 127:4, 128:15,	128:22, 129:2, 129:13, 138:13, 138:19 methods 89:5, 98:1, 110:11, 111:3, 111:19, 113:10, 113:13, 113:16, 113:19, 126:14, 127:20, 128:8, 137:22 mexico 2:13 mi 104:3, 104:14, 104:17, 105:8, 106:15 micro 63:4, 81:10 micro-level 62:12, 62:17, 63:3, 63:9, 63:17, 67:15, 67:18 microdata 60:15, 61:21, 62:2, 62:5 mid 25:1 middle 39:1, 39:2, 87:12, 87:16, 97:8, 116:12, 136:14 might 15:17, 16:14, 18:18, 22:7, 33:9, 47:22, 49:6, 49:7, 49:17, 50:11, 51:9, 57:11, 58:10, 58:13, 58:14, 63:4, 68:16, 76:5, 78:17, 82:18, 84:11, 90:3, 100:20, 104:14, 104:17, 104:19,	114:7, 143:15, 143:18 minimize 44:7 minneapolis 3:16 minnesota 3:16 minute 127:3 minutes 139:13, 144:7 mismatching 45:19 miss 104:14 missouri 2:12 mistaken 99:15 model 43:7, 43:8, 66:9, 66:20 monotonically 15:4 more 14:10, 15:1, 17:13, 17:16, 17:19, 19:11, 20:17, 25:19, 31:1, 35:20, 47:21, 56:15, 57:10, 60:2, 75:20, 81:12, 84:8, 84:17, 84:19, 85:1, 88:4, 91:21, 92:5, 104:10, 104:11, 111:7, 111:12, 111:13, 111:16, 116:15, 118:7, 121:18, 124:7, 127:17, 130:10, 134:1 morning 6:8, 6:10 most 7:15, 51:3,	120:6 motivations 33:19 much 46:12 multiple 57:11, 92:18, 103:14 murphy 5:9, 11:20, 134:8, 135:3, 136:8, 136:13, 137:17 mutual 57:20, 60:15 mutually 57:21, 58:4, 59:1, 59:12 myocardial 104:4, 104:6, 104:13, 105:9 N name 19:2, 41:1, 41:8, 41:9, 51:5, 60:4, 68:6, 73:8, 95:11, 95:15, 95:19, 98:3, 98:12, 98:20, 99:3, 99:13, 104:15, 106:14, 129:10, 131:21, 132:2, 132:3, 134:5 name-mapping 60:5 named 97:18 names 21:14, 21:17, 21:22, 23:8, 51:10, 59:11, 59:19, 60:7, 72:16, 78:18, 79:1, 84:11, 95:21, 131:15,
---	--	--	--

142:9, 143:21 national 2:14, 2:15, 45:4 nature 74:8, 144:13 ndns 59:8 necessarily 24:6, 43:14, 48:8, 62:19, 68:12, 75:15, 76:12, 103:4 need 6:21, 34:3, 35:20, 36:4, 37:4, 55:10, 66:16, 68:12, 70:9, 71:19, 72:5, 77:20, 100:8, 105:14, 109:17, 113:22, 117:9, 117:13, 121:3, 121:10, 121:13, 122:16, 122:18, 126:7, 130:10, 132:20, 138:2, 143:13, 144:16, 145:6 needed 29:19, 44:8, 56:9, 67:1, 77:15 neither 23:16 neonatal 13:16 network 18:17, 18:21 networking 92:1 never 41:13, 122:3, 130:7 new 2:13 next 46:9, 97:15,	136:15, 142:13, 145:3 nicholas 3:10, 60:9 nick 60:8 nickname 59:20 nist 44:20, 45:2, 97:14 non 120:10 noncovered 71:18, 130:14 none 125:6 nonmonotonic 14:21 nonmonotonicity 15:12 nonpreferred 83:2 normalization 61:4, 61:6, 106:20, 107:2, 107:12, 108:10 normalizations 60:22 normalize 107:9 normalized 105:3, 106:1, 108:6, 108:14, 108:19 normalizes 103:13 normalizing 18:7, 18:10, 18:12, 18:18, 18:22, 105:4, 106:5, 106:7, 106:10, 107:1 notarial 147:2 notary 2:16, 146:1, 146:3, 147:9	notes 8:14, 8:17, 9:2 nothing 52:10 notice 2:10 novel 51:3 november 1:16, 146:15, 147:3 number 4:3, 4:15, 5:3, 64:17, 65:13, 65:14, 68:7, 73:13, 73:16, 98:4, 98:13, 98:21, 99:4, 129:10, 136:1, 136:4, 136:10, 136:21, 137:10 numerous 79:10, 79:15 nw 3:5 O obfuscate 138:8 obfuscating 137:3 obfuscation 134:15, 134:17, 138:1, 138:13 object 7:5 objection 19:5, 22:2, 27:18, 32:2, 35:10, 56:5, 69:4, 69:5, 70:3, 70:20, 71:20, 82:5, 82:20, 107:7, 116:17, 116:21, 122:7, 140:15, 141:18, 142:11, 143:4, 143:22,	144:18 obtain 97:5, 135:10 obtaining 135:12 occurred 146:14 odds 109:6, 109:9 offering 13:10 office 1:1, 70:5, 70:10, 73:17, 119:9, 119:12, 119:22, 120:3, 120:7, 121:13, 121:14, 121:22, 122:1, 122:2, 122:5, 122:11, 123:5, 124:10, 124:16, 129:21, 129:22, 130:5 often 7:15 oh 52:10 okay 7:14, 10:14, 12:8, 14:20, 21:4, 25:19, 30:15, 32:18, 34:7, 38:15, 40:3, 50:18, 50:21, 51:19, 53:20, 54:22, 57:17, 59:16, 61:19, 64:1, 66:5, 72:6, 72:13, 74:1, 78:1, 79:7, 81:2, 83:11, 85:5, 86:21, 87:10, 87:18, 89:3, 89:16, 90:8, 93:15, 94:16, 98:9, 99:21, 102:4,
---	--	---	--

103:11, 107:17, 108:22, 110:4, 110:7, 113:8, 114:3, 114:15, 115:17, 115:20, 117:18, 120:22, 126:11, 131:3, 132:7, 133:2, 133:13, 134:10, 134:13, 137:18, 137:21, 139:21, 140:6, 141:20, 142:14 oklahoma 2:12 old 91:17 oliver 3:3, 4:7, 4:9, 6:7, 39:19, 39:22, 69:8, 69:17, 69:19, 72:7, 72:10, 87:2, 87:7, 115:10, 115:14, 118:15, 139:1, 139:5, 139:10, 139:15, 140:15, 141:18, 142:11, 143:4, 143:22, 144:4, 144:19, 145:2 oncology 13:16 one 7:12, 8:13, 15:1, 15:7, 19:15, 19:18, 20:15, 20:18, 28:4, 29:18, 31:18, 33:5, 33:18, 33:20, 33:22, 38:11, 48:6, 51:3, 52:20, 53:4, 55:21, 56:7, 56:8, 56:10, 58:7, 58:8,	60:11, 61:5, 62:18, 63:5, 63:7, 66:6, 67:20, 70:15, 71:5, 71:9, 71:16, 73:4, 78:12, 78:21, 80:2, 80:3, 88:4, 88:5, 93:5, 97:13, 101:3, 103:2, 104:3, 104:7, 104:16, 104:17, 105:9, 105:14, 106:13, 109:12, 110:16, 111:5, 121:7, 121:19, 123:18, 123:21, 125:17, 130:4, 131:18, 132:12, 133:22, 134:19, 135:16, 136:22, 138:8 one-way 38:10, 53:22, 54:3, 54:11, 97:5 ones 29:9, 43:14, 104:14, 104:15, 125:1, 125:19 only 6:22, 28:16, 39:5, 73:3, 76:3, 99:2, 104:17, 129:19, 137:12, 143:10 open 9:5, 105:15 operations 118:10, 126:17 opine 114:1 opinion 32:15, 35:8, 112:17, 128:14 opposite 109:11	option 45:6 options 83:19, 83:21, 93:5 order 59:4, 69:1, 90:18, 145:6 orders 145:1 ordinary 7:17, 7:22, 27:13, 27:16, 29:14, 33:12, 60:17, 62:16, 83:4, 83:17, 88:15, 113:20, 128:6 organization 92:2, 93:1 organizations 17:22, 19:17, 92:9, 92:14, 92:16, 92:17, 116:9, 129:8 organized 90:12, 91:22 original 65:22, 77:18, 81:10, 120:1, 120:5, 121:8, 122:14, 122:21, 123:1, 123:6, 125:1, 125:10, 126:3, 126:4 originals 125:14, 125:16 orthopedist 92:20, 92:22 other 6:22, 14:4, 16:15, 19:2, 19:19, 20:9, 24:3, 25:21, 44:22, 51:2, 58:21, 60:5, 60:18, 73:14, 78:13, 80:9,	82:15, 83:19, 83:20, 84:19, 88:5, 95:12, 95:15, 98:1, 98:2, 102:11, 102:15, 102:21, 103:7, 106:11, 109:7, 120:17, 125:16, 138:22 others 78:21, 79:1, 119:15 otherwise 8:3, 24:9, 32:14, 146:21 out 6:12, 8:22, 9:20, 28:17, 44:13, 45:18, 46:15, 46:22, 68:5, 68:11, 68:21, 95:15, 111:5, 111:10, 111:17, 112:8, 112:10, 112:15, 112:19, 113:6, 121:7, 123:7, 123:16, 125:2, 129:11 outcome 146:22 outlined 129:6 output 37:17, 37:21, 38:13, 45:17, 46:8, 49:16, 123:13 outside 42:4 overall 79:22 override 113:2, 113:3 own 70:10, 70:11 owner 1:9, 3:9,
--	--	--	--

146:11 owner's 5:11	part 15:2, 28:10, 34:15, 52:6, 58:11, 58:12, 78:3, 78:7, 79:4, 92:2, 118:16, 120:20, 125:8, 136:14, 142:17, 143:7, 143:10 partial 143:20 participants 52:21, 52:22, 89:7 participating 66:12 particular 48:15, 49:2, 62:21, 62:22, 63:5, 64:17, 65:12, 65:15, 68:9, 68:13, 73:17, 90:3, 91:13, 100:19, 100:20, 101:5, 106:22, 107:21, 110:21, 114:11, 131:19, 135:16 parties 15:1, 15:5, 15:7, 53:6, 53:10, 53:15, 71:15, 101:15, 146:18, 146:20 parts 99:4 party 15:14, 22:4, 22:8, 23:11, 23:14, 30:20, 33:20, 52:14, 52:19, 52:20, 53:5, 120:18, 132:15, 146:10 passage 140:7, 140:14, 141:9, 142:3,	142:8, 143:19 passages 141:14 passing 26:22 paste 47:1 patent 1:1, 1:3, 1:9, 1:12, 3:9, 4:16, 4:18, 4:20, 5:4, 5:7, 5:11, 8:21, 10:9, 10:11, 10:15, 22:20, 23:9, 25:16, 25:19, 27:11, 28:8, 28:10, 28:12, 29:10, 29:11, 29:14, 30:11, 30:14, 31:16, 32:4, 35:3, 35:9, 38:8, 48:9, 55:21, 81:8, 82:3, 82:18, 100:16, 109:21, 127:21, 146:11 patents 8:9, 8:21 pathology 13:16 patient 19:20, 20:1, 21:21, 49:22, 51:10, 63:6, 63:11, 63:19, 65:5, 70:6, 73:16, 78:18, 81:10, 85:20, 86:9, 90:1, 90:3, 91:20, 93:18, 94:2, 94:19, 94:20, 95:4, 95:5, 95:11, 95:12, 95:21, 96:5, 96:9, 98:3, 98:12, 99:9,	100:1, 100:2, 101:2, 101:14, 101:16, 101:20, 102:2, 116:10, 119:10, 120:1, 121:8, 123:8, 124:1, 124:9, 125:3, 126:15, 126:19, 127:13, 129:11, 129:19, 130:1, 130:18, 130:21, 131:11, 133:5 patient's 90:4, 95:19, 98:20, 130:19, 131:19, 131:21 patient-identify- ing 85:13 patient-level 89:18, 89:22, 90:2, 94:12 patients 47:16, 47:18, 48:2, 48:6, 48:12, 48:16, 48:21, 49:3, 49:4, 49:6, 65:3, 66:11, 66:21, 86:4, 86:5, 92:18, 94:13, 99:13, 101:5, 101:9, 101:10, 101:11, 114:11, 117:11, 123:12, 123:15, 124:10, 125:7, 131:16, 136:1, 136:5, 136:10, 136:21, 137:1, 137:11, 137:12 patterns 111:15 pc 3:12 pcp 102:8
----------------------------------	---	--	--

pdf 9:4 peeled 77:7 pending 7:1 people 49:18, 104:12 people's 68:10 perform 45:14, 55:22, 56:4, 56:9, 67:1, 68:16, 74:17, 81:13, 100:22, 101:3, 135:14 performed 33:7, 47:14, 100:11, 118:9, 118:16, 122:12 performing 66:18, 67:19, 81:17, 96:3, 101:1, 103:21 performs 124:14 perhaps 15:20, 21:16, 53:3, 65:4, 75:20 period 13:14 persistent 56:11 persistently 96:18 person 7:16, 7:21, 27:12, 27:16, 29:5, 29:7, 29:13, 33:12, 55:3, 55:12, 55:13, 55:17, 56:11, 57:9, 60:9, 60:17, 62:4, 62:16, 73:4, 81:11,	81:15, 83:3, 83:17, 88:15, 99:15, 110:17, 110:20, 113:20, 128:6, 135:16, 137:10, 141:5 person's 19:2, 41:1, 41:8, 99:2 personal 30:21 personally 21:13 personnel 102:10 perspective 7:16, 8:5, 72:21, 92:1 perturbation 134:18, 134:22 petition 8:9 petitioner 1:6, 3:2 petitioner's 139:22 pharmaceutical 47:17, 49:5, 49:10, 102:9 pharmacies 55:17, 56:3, 56:10 pharmacy 64:10 phd 1:15, 2:1, 4:6, 6:2, 146:4, 146:14 physician 64:8, 64:9, 64:11, 64:13, 64:14, 64:18, 65:4, 65:8, 65:18 physician's 70:5, 73:17 physician-level 64:3, 64:6,	65:1 pi 14:9 pick 43:9, 45:13 pid 95:3, 97:1, 97:4, 97:6 pids 94:19, 96:16, 98:2 piece 46:22, 62:3, 62:7, 65:16 pii 23:11, 129:10 pipe 76:4 place 23:10, 29:4, 29:12, 40:20, 77:19, 88:19, 107:2, 107:4 places 39:15, 39:16, 79:20, 79:21 plain 42:11, 42:12, 42:16, 42:21, 42:22, 43:1, 43:3, 43:8, 43:10, 43:11, 43:13, 43:19, 44:1, 44:6, 44:12, 44:14, 45:8, 45:11, 45:19, 46:3, 46:13 play 80:21 plaza 3:13 please 7:12, 8:3, 34:6, 47:19, 50:19, 93:14, 103:10, 114:14, 133:12, 134:9,	139:13 point 6:22, 18:4, 30:8, 32:14, 75:16, 75:21, 82:7 pointed 107:15 policy-oriented 17:13, 17:19 pool 49:22, 50:4, 65:2, 89:6 population 48:3, 51:1, 60:5, 100:11, 100:12, 100:13, 100:22 portion 46:15 portions 140:8 posa 7:21, 26:1, 26:4, 26:18, 28:14, 61:5, 61:12, 67:20, 75:14, 86:2, 89:21, 90:17, 128:10, 133:20, 141:13, 142:9 posa's 8:5, 55:8, 62:1, 72:21, 86:10, 98:15, 140:12, 141:8 position 119:2, 126:22 positioned 49:6 possible 21:16, 27:14, 100:21, 123:5, 143:11, 145:3 post-dated 15:16 potential 89:7
---	---	--	---

potentially 137:6 pre 37:16 pre-image 37:22, 38:1, 38:5, 38:13 pre-images 37:19 preclude 31:12 preclusion 32:8 predefined 66:11, 66:22 prefer 81:12 preferably 83:14, 83:18 preference 81:4, 81:7, 83:5, 83:7 preferred 82:1, 82:3, 82:6, 82:14, 82:18, 83:1 prefix 59:20 premise 65:7 prepare 8:6, 8:7 preparing 61:10 prescribed 65:15, 124:13 prescriber 64:11 prescription 56:12 prescriptions 64:17, 64:19, 65:13, 65:14 present 88:10, 88:22, 102:8 preserve 68:5	pretty 97:19 prevent 27:5, 28:13, 28:15, 29:15, 46:3, 46:12, 130:13, 135:11, 136:20 preventing 18:16 preventions 29:4 prevents 27:21, 28:6, 29:4, 30:3, 30:20, 52:11 previous 15:2 previously 84:1 primary 12:18, 13:3, 92:20 primitive 37:15 principle 14:9 printed 8:22 prior 8:10, 8:22, 12:20, 14:1, 111:18 pristine 9:1, 9:6 privacy 17:1, 53:15, 67:8, 68:2, 68:6, 84:20, 84:21, 85:1, 85:22, 100:3, 101:16, 101:20, 126:19, 130:18 private 117:3, 122:1, 141:11 privilege 7:6, 144:18	probably 43:20, 46:1, 57:20, 60:20, 61:14 problem 19:6, 19:12, 19:14, 20:3, 20:9, 23:1, 30:16, 105:17 procedures 106:13 proceedings 145:8 process 26:12, 36:19, 54:18, 67:7, 96:4, 97:19, 110:15, 111:21, 112:4, 122:9, 131:5 processes 77:14, 113:10, 113:13, 113:17, 113:19 processing 131:6 processor 80:4 processors 80:12 produce 24:1 produced 32:20, 92:21 produces 37:17 products 102:11, 102:15, 103:7, 115:7 professional 2:15 professionals 16:22 professor 12:21 program 15:18, 16:21, 17:5, 17:8,	17:10, 66:12 project 19:15, 20:6 projects 12:22, 13:4, 13:12, 13:22, 14:2, 14:8, 14:10 proper 28:21, 47:3, 47:7 properly 52:22, 111:2 property 37:18, 37:20 proposed 118:21 propounded 6:4 protect 54:17, 75:16, 76:3, 76:4, 76:6, 76:7 protected 117:3 protecting 126:19, 130:6 protocol 15:2, 15:6, 15:10, 16:13, 51:4, 52:6, 52:21, 76:19, 80:10, 91:5, 91:7, 91:15, 91:18, 92:11, 93:3 protocols 14:21, 14:22, 15:3, 16:14, 74:15, 76:3, 91:9 provide 66:10, 66:20, 76:16, 89:5, 103:22, 112:3 provided 86:4, 91:18, 136:8
--	--	---	--

	Q	R	
provider 92:20, 104:16, 104:18 providers 92:18 provides 47:8, 48:9, 86:3, 132:16 providing 14:11, 21:21, 32:19 public 2:16, 28:1, 30:10, 115:22, 116:8, 117:3, 121:22, 126:17, 146:1, 146:3, 147:9 public-key 98:18 publication 4:21, 5:5 pulaski 147:10 pull 25:16, 35:21, 103:19 pulling 32:11 pump 102:18 purpose 23:19, 23:22, 56:22, 110:21, 115:5, 133:21 purposes 79:19, 126:16 pursuant 2:10 pursue 13:2 put 29:4, 58:18, 71:1, 122:15, 134:2 puts 46:15 putting 18:19, 70:15	qualify 35:2, 35:8, 35:19, 103:3 quality 74:9 quantifies 49:18 queries 50:14, 100:15, 103:21, 108:6, 108:19, 111:15 query 49:2, 49:7, 49:20, 50:3, 51:9, 51:13, 57:19, 57:20, 66:7, 72:15, 86:3, 100:18, 107:4, 107:10, 107:13, 108:8, 108:10, 135:19, 135:22, 136:7, 138:14, 138:15 question 7:1, 7:2, 8:4, 14:2, 22:13, 31:9, 32:13, 37:6, 42:17, 42:19, 51:13, 53:9, 69:4, 70:4, 71:12, 82:13, 85:16, 85:17, 87:1, 94:2, 98:14, 111:7, 127:8, 129:16, 136:21, 143:16, 144:17 questioning 144:5, 144:6 questions 6:4, 7:7, 7:10, 7:12, 7:15, 72:3, 139:11, 139:14, 144:2, 144:20 quite 91:16, 139:2	raised 105:3 ran 16:5 random 45:12, 45:14, 45:16 range 137:5 rather 55:8, 83:8, 136:20, 137:12 raw 67:7 rbc 3:13 re-identification 119:5, 122:4, 125:12, 125:21, 127:13 re-identify 77:12, 122:13, 129:22, 130:20 re-identifying 126:15 re-read 8:7 read 32:6, 51:11, 55:10, 63:12, 66:16, 75:11, 80:1, 80:17, 85:15, 100:8, 109:17, 116:7, 128:10, 142:15, 142:18 readable 133:16, 133:21, 134:1 reading 29:14, 31:22, 113:21, 128:6 reads 80:9, 87:19, 102:7 realize 90:10	really 26:6, 59:2, 59:13, 105:8, 105:15, 130:10 reason 6:13, 7:11, 16:16, 84:5, 84:14, 99:7, 104:7, 108:15, 116:5, 120:14, 129:5, 130:4, 133:22 reasonable 119:19 reasoning 15:8 reasons 58:21, 67:9 recall 18:5, 41:17, 41:18, 42:2, 42:5, 42:9, 139:22, 140:19, 141:22, 142:20 receive 27:3, 43:10, 92:21, 107:10, 145:7 received 77:6, 92:10 receiver 27:2 receives 76:1 receiving 86:16, 107:4 recipient 76:9, 76:10, 77:10, 77:13 recollection 130:2 record 19:19, 45:3, 53:11, 57:10, 62:8, 62:20, 62:21, 63:3, 69:16, 72:8, 87:4, 88:12,

88:17, 90:5, 91:4, 95:11, 95:16, 104:3, 104:4, 115:11, 119:10, 119:14, 120:4, 120:5, 120:8, 122:14, 122:21, 122:22, 123:9, 124:1, 125:2, 129:18, 130:1, 139:3, 140:9, 144:21, 146:8 recorded 19:3 records 20:2, 21:17, 21:21, 22:4, 47:13, 48:1, 48:15, 49:22, 53:14, 56:9, 58:10, 58:13, 60:10, 61:7, 62:12, 62:15, 62:17, 63:9, 63:11, 63:17, 63:18, 65:6, 67:14, 70:7, 70:15, 70:17, 71:16, 80:4, 84:13, 86:4, 88:20, 91:1, 91:9, 91:20, 91:22, 92:8, 92:10, 92:14, 92:19, 92:21, 93:2, 93:8, 93:22, 94:12, 101:4, 110:9, 111:6, 111:19, 113:14, 120:1, 120:11, 121:6, 121:7, 121:9, 121:11, 121:14, 122:6, 122:17, 123:6, 123:11, 123:17, 123:18, 123:19, 124:9,	124:14, 124:22, 125:1, 125:10, 126:1, 126:3, 126:4, 129:8, 130:19, 130:20, 131:5, 131:12, 131:20, 135:14 recover 16:6 recovered 16:9 redirect 139:14 reduce 44:7 reduced 67:8 refer 7:21, 10:14, 12:11, 14:14, 16:20, 36:14, 37:9, 38:16, 103:13, 106:11, 142:13 reference 10:18, 11:2, 11:8, 11:14, 11:20, 31:4, 50:16, 51:20, 56:18, 57:19, 61:20, 62:12, 63:8, 63:16, 64:3, 87:9, 87:12, 89:18, 94:18, 96:3, 97:8, 107:8, 109:18, 110:2, 110:6, 115:16, 115:22, 133:3, 134:8, 139:20 referenced 20:7, 44:17 references 8:10, 8:22, 53:21 referred 13:5, 98:16, 135:8	referring 17:5, 22:8, 38:21, 42:1, 42:12, 50:2, 50:4, 62:6, 63:10, 63:17, 75:22, 82:8, 84:7, 86:12, 118:20, 141:10, 144:10 refers 34:8, 73:6, 73:7, 74:3, 81:4, 82:1, 82:6, 103:20, 104:3, 104:4, 113:9, 135:4, 140:7, 140:22 refilling 56:12 regard 107:20 regardless 75:1, 142:3 register 20:17 registered 2:14, 2:15, 69:4 registration 20:15 regulation 75:19 regulations 126:18 reidentify 35:8, 111:16, 117:11, 118:5, 121:14, 121:21, 122:17, 124:16, 129:18 related 14:3, 59:2, 65:3, 146:17 relates 88:11 relating 57:11	relation 71:21 relationship 25:13, 25:22, 26:2, 26:7, 80:11 relative 7:16, 8:5, 76:22 release 41:8 released 21:12, 22:4, 141:1 relevant 49:21 rely 76:19 remained 119:12 remains 77:9 remember 13:6, 13:7, 20:8, 20:21, 63:14, 92:15, 93:4, 132:21 remote 15:19 remotely 1:14 remove 113:1 removed 95:13, 125:8 removing 110:13, 111:8, 112:20 rephrase 136:19 replace 105:9 replaced 95:13, 95:14 replacing 133:15 reply 6:4
--	---	---	---

report 23:8, 33:6, 37:3, 61:11, 114:1, 118:17, 127:2, 127:3 reported 1:22, 33:3 reporter 2:11, 2:15, 2:16, 4:11, 45:2, 69:15, 135:2, 144:22, 145:4, 146:1, 146:2 repository 50:8, 50:11 representations 20:1 represented 146:11 reproducibility 129:17 reproducible 133:4 reproducibly 36:15 request 21:15, 21:20, 22:13, 23:12, 24:1, 24:2, 27:2, 27:6, 31:4, 31:8, 86:15, 108:13, 114:4, 114:10, 138:10 requested 22:1 requester 21:22, 22:5, 31:13, 31:20, 32:10, 84:12, 85:12, 85:19, 86:16, 108:7, 108:8 requesting 123:3 requests 22:12	require 114:18, 118:7 required 7:6, 110:12 requirement 83:5, 83:6, 86:18, 119:6, 119:18 requirements 33:22, 35:22, 86:11, 119:5, 127:1, 129:12 research 12:11, 12:15, 12:16, 22:9, 37:4, 72:4, 102:9, 102:19, 113:15, 114:1, 117:13, 118:8, 126:7, 126:16, 127:7, 127:17, 130:11 researcher 68:8 resistant 44:12 resolution 65:19, 65:21, 66:8, 67:3, 67:8, 67:17, 68:15, 70:2, 70:19, 81:12, 81:17, 81:19 respect 18:21, 26:3, 54:12, 73:16, 74:13, 84:18, 84:20, 86:11, 106:20, 107:12, 127:5, 128:19, 129:17 respecting 100:2 respective 57:22 response 5:12, 86:3, 86:7, 136:22,	137:3 restate 85:17 result 138:10 resulted 123:12, 123:13 results 50:3 retain 87:20 retaining 96:4 returning 101:10 reveal 40:10, 41:7, 41:10, 100:12 revealed 105:18 reverse 35:15, 121:2, 121:3, 122:18, 123:20, 124:4 reversed 35:5, 36:19, 80:13, 80:21 reversible 80:13, 120:12, 120:20 reversing 21:18, 35:18, 36:3, 36:6, 120:15 review 117:9 reviewed 141:15 richardson 3:12 right 8:1, 41:20, 49:9, 52:1, 59:10, 67:12, 87:16, 94:14, 98:18, 100:21, 109:3, 111:9, 112:11, 113:11,	121:2, 131:13, 134:7, 135:16, 136:6, 139:15, 143:3 risk 47:16, 48:2, 48:10, 115:6 rmr 1:22 robust 58:19 roles 80:20 rounding 18:18 routinely 114:18 rpr 1:22, 147:8 rsa 98:18, 98:21 rubin 1:15, 2:1, 4:6, 5:10, 6:2, 6:8, 40:1, 72:11, 87:8, 115:15, 118:14, 139:6, 144:5, 144:16, 146:4, 146:14 rule 35:14, 35:22, 121:17, 124:6 rules 121:20, 130:8 run 15:18, 16:8, 16:10 running 17:8
S			
safeguard 47:8 said 14:2, 19:10, 19:11, 35:11, 35:14, 42:16, 45:2, 55:14,			

78:22, 87:2, 94:9, 100:18 salary 46:22, 47:1 salt 45:7, 45:11, 45:14, 45:16, 45:18, 45:22 same 9:5, 9:8, 19:20, 20:1, 26:10, 31:14, 32:9, 36:13, 36:20, 36:21, 36:22, 37:20, 45:15, 46:1, 50:11, 50:15, 52:4, 52:13, 53:15, 54:3, 55:12, 55:17, 56:13, 57:12, 60:9, 63:8, 63:11, 63:18, 67:2, 73:5, 84:16, 88:21, 91:12, 99:9, 99:11, 99:13, 99:15, 100:2, 105:8, 105:10, 117:15, 123:13, 123:20, 124:2, 127:9, 130:21, 132:15, 135:18, 137:4, 137:6 satisfy 50:13, 73:4, 127:5, 128:16, 129:14, 129:16 say 12:15, 14:1, 16:5, 18:15, 19:17, 23:14, 28:6, 32:3, 33:15, 35:4, 38:2, 44:13, 45:13, 46:17, 54:20, 57:8, 57:21, 62:20,	68:8, 68:21, 69:11, 70:4, 70:13, 70:21, 75:21, 76:7, 79:2, 81:15, 82:6, 84:17, 86:1, 86:12, 95:14, 102:17, 106:15, 108:17, 118:21, 122:1, 123:15, 134:20, 137:13, 137:15 saying 21:10, 27:7, 29:7, 29:21, 32:4, 35:13, 66:19, 67:6, 70:14, 80:18, 108:5, 108:9, 108:11, 116:8, 137:7, 137:13, 138:7, 138:19 says 6:4, 41:6, 51:8, 52:14, 55:21, 60:3, 60:14, 65:8, 73:18, 76:15, 78:2, 103:6, 104:1, 104:3, 104:10, 106:1, 110:15, 110:19, 114:16, 116:2, 116:11, 126:12, 131:9, 138:12 scenario 27:10, 27:17, 30:6, 49:14 schneier 97:18 school 13:7, 13:15, 17:21, 20:11, 20:12, 20:13 scope 27:18, 35:10, 122:7, 140:15 score 23:10, 48:10,	48:20, 49:1 screen 50:18 seal 147:2 search 44:8, 44:9, 44:16, 47:14, 47:17, 48:1, 48:6, 58:22, 67:14, 67:16, 81:22, 88:11, 101:3, 104:11, 106:21, 107:1, 107:5, 114:10, 118:17, 132:1, 135:14 searchable 58:18, 103:19 searched 50:5, 95:19, 131:20 searches 50:9, 67:19 searching 47:12, 48:22, 58:3, 58:10, 58:20, 59:2, 59:3, 68:14, 81:10, 81:14, 81:17, 84:12, 88:17, 89:5, 101:5, 101:8, 101:10, 104:10 second 38:17, 94:18, 96:2, 102:5, 102:6, 105:14, 114:16, 135:3, 136:14, 137:19 secondary 83:2 secret 105:18 section 52:13, 74:21, 104:22, 107:15, 127:3, 131:4	secure 13:12, 16:16 security 12:12, 12:19, 13:9, 13:20, 15:10, 16:12, 17:1, 17:17, 17:22, 25:7, 28:15, 68:7, 73:13, 74:9, 75:14, 75:20, 76:20, 98:4, 98:13, 98:21, 99:4, 129:10, 143:12, 143:15 see 8:18, 12:13, 16:7, 17:2, 19:6, 21:6, 22:21, 23:6, 23:7, 31:10, 32:11, 32:12, 32:21, 34:11, 37:11, 38:18, 40:6, 40:12, 50:6, 51:22, 52:16, 54:1, 55:5, 55:6, 56:16, 56:20, 58:1, 59:21, 62:13, 64:4, 65:17, 66:13, 72:19, 72:20, 73:9, 74:6, 74:11, 74:21, 75:5, 75:6, 76:14, 78:5, 79:13, 80:14, 80:15, 81:5, 81:12, 83:15, 83:20, 85:9, 87:22, 88:13, 89:8, 89:19, 90:14, 92:18, 93:19, 96:6, 96:19, 98:5, 98:9, 100:4, 100:5, 102:12,
---	--	---	--

103:15, 106:3, 107:22, 108:1, 114:20, 116:3, 116:4, 117:7, 117:21, 126:1, 126:20, 128:21, 132:10, 133:7, 133:18, 133:19, 134:19, 135:6, 135:20, 136:16, 138:4, 138:16, 140:10, 141:6 seem 31:12 seemed 69:20 seems 31:22, 40:22, 68:18, 75:7, 135:13 selected 97:20, 107:20 selection 97:19 selling 115:6 seminars 14:11 send 16:2, 16:9, 25:20, 27:2, 87:20, 108:18 sending 75:17, 93:17 sends 95:16 sense 88:8, 93:12, 120:12, 122:20 sensitive 76:18, 84:8, 84:18, 85:1, 143:12, 143:15 sent 33:6, 57:19, 88:5, 95:6, 120:19, 138:10, 141:11	sentence 34:8, 55:2, 78:2, 79:8, 80:8, 83:12, 87:13, 87:19, 88:10, 90:9, 92:3, 96:2, 98:7, 99:22, 101:13, 102:5, 102:6, 109:1, 113:9, 114:16, 126:12, 127:6, 127:10, 128:7, 136:15 sentences 96:15 separate 26:8, 31:20, 60:10 served 138:2 server 15:20, 16:3, 16:9, 23:5, 23:15, 23:16, 23:18, 23:20, 23:22, 25:5, 25:8, 25:10, 25:15, 26:2, 26:5, 27:3, 27:5, 27:8, 27:21, 28:3, 28:9, 28:17, 29:3, 29:16, 30:9, 31:13, 31:19, 32:9, 38:22, 39:1, 39:2 servers 70:11, 79:22 services 67:11 serving 9:16 set 66:1, 66:8, 91:7, 92:17, 124:19, 146:5,	147:1 sets 106:16 settimi 4:22, 11:2, 87:8, 88:9, 88:21, 89:4, 89:15, 90:7, 93:13, 93:16, 94:15, 94:19, 94:20, 95:1, 96:2, 96:14, 96:16, 98:2, 99:20, 101:8, 101:19, 102:3, 102:16, 103:20, 104:1, 105:2, 105:12, 107:16, 107:19 settimi's 101:3 several 57:7, 141:4 share 26:6, 26:13, 69:1, 70:8, 70:11, 101:19 shared 70:17, 71:3, 71:18, 92:9, 92:14, 92:19, 101:15, 102:1, 119:14, 122:3 sharing 27:22, 30:9, 91:9, 93:3 short 133:16 shorthand 2:11, 146:1 should 21:12, 28:16, 30:9, 57:8, 57:21, 68:5, 68:20, 68:21, 75:3, 85:12, 85:19, 86:4, 86:8, 86:17,	105:18, 108:17, 118:5, 125:9, 142:5 shouldn't 121:21 show 67:4, 100:18, 101:7 showed 124:4 showing 9:4 shown 39:7 shows 31:19, 33:6 side 77:10, 77:13 signature-b7fzp 147:6 silly 121:10 similar 59:19, 60:15, 61:7, 73:20, 91:20 simply 125:3, 126:22 since 122:5 single 56:15, 124:1 sit 36:10, 61:14 site 67:19 sites 39:11, 39:17 sitting 37:5 situation 55:20, 57:5, 124:21 situations 99:12 six 107:18 sizes 59:10
---	--	--	--

skill 7:17, 7:22, 27:13, 27:16, 29:14, 29:18, 33:12, 60:17, 62:16, 83:4, 83:17, 88:15, 113:20, 128:6 slice 78:22 small 62:7, 62:18 social 68:7, 73:13, 98:4, 98:12, 98:20, 99:3, 129:10 software 28:20 solely 76:19 solution 15:22, 16:1, 33:19 solutions 29:1 some 6:21, 8:20, 8:21, 9:5, 16:15, 17:16, 18:4, 22:11, 23:9, 23:21, 26:19, 37:4, 40:20, 43:16, 43:21, 49:17, 54:16, 63:12, 65:22, 72:4, 76:21, 78:3, 78:10, 80:19, 83:2, 84:19, 100:8, 111:3, 112:9, 113:22, 117:2, 122:1, 122:10, 135:1, 142:16, 143:14 somebody 16:4, 22:5 somebody's 20:17	somehow 68:19 someone 21:12, 21:20, 27:5, 34:19, 55:11, 62:21, 70:8, 78:12, 129:18 someone's 123:2 something 18:8, 27:19, 28:10, 33:9, 36:9, 42:22, 46:13, 53:12, 61:11, 62:8, 69:11, 73:2, 83:1, 83:6, 83:7, 85:1, 88:18, 100:20, 109:6, 109:8, 109:10, 127:16, 128:12, 134:6 sometime 13:14 somewhere 25:3, 81:21, 99:10 sorry 69:6, 82:11, 108:3, 116:18, 134:20 sort 22:11, 23:21, 24:17, 26:19, 29:13, 39:9, 40:20, 65:2, 93:2, 109:11, 111:10, 112:3, 122:2 sounds 7:3, 35:13, 87:5, 94:14 source 39:11, 39:17, 57:22, 58:7, 58:9, 59:3, 60:6, 67:19, 68:14, 76:2, 80:4, 80:12, 80:20, 81:20, 104:17, 104:19, 109:19, 119:9, 141:1 sources 57:3, 58:17, 59:5, 71:1, 71:2, 93:22, 94:4, 103:14, 140:7 south 3:14 space 13:21, 44:8 speak 128:1, 128:3 speaking 52:8, 83:3 specific 18:14, 21:20, 32:8, 48:1, 48:6, 48:11, 48:21, 51:5, 51:10, 51:14, 60:15, 65:5, 73:8, 78:3, 100:13, 108:9, 110:10, 111:20, 112:4, 112:18, 118:6, 118:12, 121:20, 124:7, 125:5, 125:13, 126:2, 127:5, 129:5, 129:13, 129:15, 129:16, 137:11, 138:20, 142:16 specifically 13:6, 14:6, 14:16, 19:11, 23:20, 30:13, 42:5, 50:2, 73:6, 73:22, 76:8, 82:22, 94:17, 96:2, 116:15, 118:19, 130:8 specification 31:21, 32:7 specifics 35:20, 63:4, 72:16 specifying 8:3 spot 118:1 spread 68:8, 68:13 ssh 74:15 ssl 74:16 staff 102:8 standard 44:20, 54:6, 74:15, 97:15, 119:7 standardization 90:21, 90:22, 93:9, 93:10 standardizations 91:6 standardized 90:13, 92:6 standards 45:5, 68:2, 119:4 standing 145:1 stands 44:19 start 6:11, 12:4, 12:16, 37:21, 139:19, 144:6 started 12:17, 36:21, 123:21 starting 12:22, 13:19, 32:17, 50:20, 51:18, 56:14, 57:16, 59:15,
---	--

61:18, 62:11, 63:22, 65:7, 66:4, 72:12, 77:21, 79:6, 80:7, 83:13, 115:18, 126:9, 127:11, 131:2, 132:22, 133:12 state 2:16, 45:2, 74:8, 88:22, 146:3 stated 40:9 statement 88:2, 90:16, 100:7, 116:1, 116:6, 127:18, 138:18 states 1:1, 2:12, 4:16, 4:18, 4:20, 5:4, 5:7, 32:19, 34:3, 35:15, 50:22, 55:3, 57:6, 66:6, 72:14, 88:10, 89:4, 90:10, 99:22, 101:13, 107:19, 137:22 statistically 123:4 staying 22:18 step 33:1 stephens 3:10, 4:8, 19:5, 22:2, 27:18, 32:2, 35:10, 56:5, 69:3, 69:12, 69:14, 70:3, 70:20, 71:20, 82:5, 82:20, 107:7, 116:17, 116:21, 118:12,	122:7, 139:12, 139:18, 144:2, 144:11, 144:16, 144:21, 145:5, 145:6 steps 74:4 stick 15:19 still 16:15, 17:8, 34:20, 71:21, 96:4, 98:7, 112:12, 122:22, 137:2 store 39:15, 59:9, 93:2, 93:22, 97:6, 131:11 stored 25:3, 93:7, 94:3, 104:8 street 3:14 strike 143:15, 143:18 string 134:2 strings 133:16, 133:21 strip 112:8 stripping 111:5, 111:10, 111:17, 112:14, 112:18, 113:6 stronger 75:4, 76:16, 76:22, 84:2, 84:6, 84:9, 84:15, 142:6 structure 60:16 students 20:12 studied 49:13 study 47:18, 49:7,	49:19, 68:8, 89:7, 100:17, 100:22 style 4:3 subject 71:3, 75:18, 114:5, 114:7 submissions 97:16 substance 139:7 substeps 80:3 subtract 45:18 suffering 96:12 suffix 59:20 suggest 142:9 suggested 98:19 suggesting 75:7, 75:13 suggests 28:10 suite 3:15 summarize 119:8 summary 15:22 super 77:2, 77:3, 77:7, 77:9, 77:17 support 5:11 suppose 56:1, 70:12, 78:14, 81:21, 84:7, 88:3, 108:16, 113:2, 133:22 sure 8:2, 14:16,	16:19, 26:12, 27:15, 30:12, 31:2, 34:15, 37:5, 37:14, 45:4, 63:16, 67:5, 69:3, 69:17, 82:9, 91:21, 111:1, 112:10, 113:4, 119:19, 130:7, 130:10 surrounding 51:11, 63:12, 100:8 sworn 6:3, 146:6 symmetric 97:21 symmetrical 37:1 symposium 5:9 syntax 103:20 system 12:17, 15:7, 16:16, 19:22, 21:21, 22:17, 25:5, 28:4, 29:9, 31:17, 34:2, 61:8, 67:18, 74:10, 79:22, 81:12, 88:4, 88:7, 93:18, 93:21, 99:8, 101:4, 111:20, 112:4, 131:6, 131:14, 132:9, 135:5, 135:11 systems 12:12, 12:20, 13:13, 15:9, 20:14, 87:14, 87:20, 89:5, 89:12, 126:13, 127:20, 128:8 T table 8:20
---	---	---	--

take 6:20, 7:2, 16:1, 36:18, 39:20, 46:7, 46:21, 77:19, 87:2, 97:4, 105:7, 105:15, 106:12, 107:2, 107:4, 109:12, 115:11, 117:16, 139:2, 139:12 taken 9:2, 68:5, 68:11, 68:21, 112:10, 146:8 takes 29:12, 36:9, 37:16, 46:14, 95:15 taking 6:16, 56:3, 58:16, 70:14 talk 30:18 talked 84:1, 106:13, 117:10, 132:14 talking 18:16, 22:3, 23:15, 52:5, 65:9, 84:19, 106:22, 107:12, 111:20, 117:2, 120:14 talks 67:2, 80:1, 104:2, 112:20, 127:12, 127:15 taught 17:7, 17:9, 18:3, 19:8 teach 17:16, 18:20 teaches 109:2, 109:5, 109:7, 109:15, 109:18, 109:21 teaching 16:21, 17:20,	109:10, 109:13 team 102:19 technical 14:17, 14:19, 17:7, 17:14, 17:15, 17:16, 18:2, 29:1, 29:19, 29:22, 30:1 technique 18:20 techniques 28:15, 28:18 technological 90:11 technologies 90:19 technology 13:9, 45:5 tell 8:16, 14:14, 65:11, 110:10 tennessee 2:13 term 18:11, 18:22, 36:16, 40:8, 65:19, 83:14, 104:17, 105:3, 105:11, 106:8, 108:10, 109:2, 109:4, 132:8, 135:9, 141:14 terminologies 61:2 terminology 58:8, 58:9, 91:12, 91:20, 103:14, 104:19 terms 40:5, 88:5, 107:19 testimony 6:14, 6:18, 139:7, 146:9 testing 69:12	text 9:9, 42:11, 42:13, 42:17, 42:21, 42:22, 43:1, 43:3, 43:8, 43:10, 43:11, 43:13, 43:19, 44:1, 44:6, 44:12, 44:14, 45:8, 45:11, 46:4, 46:13, 51:11, 63:13, 100:8, 108:11 texts 45:19, 45:20 th 147:2 thank 6:10, 139:10 themselves 101:11 therefore 66:8, 99:13, 131:18 thereof 99:4 thesis 14:14, 14:17, 14:18, 14:20 thing 6:22, 26:4, 31:14, 48:21, 98:19, 105:8, 105:9, 105:10, 108:9, 109:7, 109:12, 132:15 things 17:9, 18:1, 18:3, 20:18, 28:20, 28:22, 63:1, 72:3, 73:20, 105:7, 106:12, 110:15, 138:22 think 9:7, 9:14, 18:14, 26:11,	29:18, 30:6, 31:15, 36:8, 52:4, 56:6, 57:8, 57:13, 65:16, 70:22, 75:13, 76:17, 78:19, 79:2, 84:20, 91:14, 91:21, 92:5, 93:6, 93:12, 97:16, 102:22, 104:20, 109:14, 111:22, 112:16, 113:20, 116:15, 116:22, 121:17, 122:16, 122:20, 124:5, 128:10, 129:2, 130:4, 130:22, 132:1 third 22:4, 22:7, 23:11, 23:14, 30:20, 52:14, 52:19, 53:5, 53:6, 53:10, 53:15, 119:18, 132:14 thought 61:16, 128:2, 128:11 three 14:8, 15:19, 99:17, 119:3, 129:12, 137:7, 137:14, 137:16 threw 123:16 through 50:8, 60:4, 67:6, 67:14, 67:17, 74:2, 74:20, 84:1, 85:8, 117:20, 130:17, 140:20, 141:21 throughout 81:9 time 8:13, 14:1,
--	--	--	--

14:5, 14:7, 14:9, 15:9, 16:8, 34:1, 45:14, 46:1, 47:11, 100:2, 113:16 times 8:12, 9:12 timing 18:17 timings 18:19 title 81:3 titled 14:21, 134:14 today 6:9, 6:14, 7:20, 8:15, 10:15, 17:8, 37:5, 139:8 today's 44:10 together 39:15, 46:11, 58:18, 58:22, 59:18, 60:3, 63:11, 63:19, 70:15, 71:1, 72:17, 72:22 token 24:4, 24:10, 24:13, 24:14, 27:22, 29:5, 29:17, 30:4, 30:22, 34:18, 35:2, 35:19, 36:21, 38:7, 40:8, 40:19, 41:21, 54:20, 95:8, 129:9, 133:9 tokenization 18:3, 35:5, 35:9, 37:2, 41:2, 41:16, 41:19, 54:17 tokenized 142:10	tokenizing 143:21 tokens 24:1, 27:2, 34:10, 34:14, 35:15, 36:1, 36:14, 36:19, 36:20, 39:6, 42:1, 54:10, 61:6, 109:22 told 29:11 top 71:13, 111:22, 117:14, 130:5, 136:8 topic 18:6 total 65:13, 65:14 tour 13:14 towards 85:6, 97:22 track 17:12, 17:13, 17:14, 17:15, 17:16, 18:2, 18:9 tracks 17:11 trademark 1:1 traditionally 24:22 transcript 4:14, 5:2, 145:7 transfer 20:12 transmission 74:17, 75:8, 75:14, 76:2, 76:9, 76:10, 76:11, 76:19, 77:1, 77:6, 77:19, 93:7 transmitted 77:5, 92:10	transmitting 74:3, 74:4, 74:14 treats 65:4 trial 1:3, 49:15 tried 20:17 true 146:8 trusted 52:14, 52:18, 52:21, 53:4, 53:6, 53:10, 53:15, 132:8, 132:13, 132:14, 132:18 truthful 6:14, 6:17 try 7:10, 7:13, 135:14 trying 48:17, 49:15, 58:21, 67:13, 136:20 turn 12:6, 20:22, 30:11, 34:5, 40:1, 50:16, 50:19, 51:17, 53:18, 54:21, 57:15, 61:17, 63:21, 66:3, 72:11, 73:21, 77:21, 79:5, 80:7, 80:22, 85:3, 86:19, 87:8, 87:11, 89:2, 89:14, 90:7, 93:13, 99:19, 102:3, 103:9, 107:16, 108:20, 110:2, 110:5, 114:2, 115:15, 115:18, 126:9, 131:1,	132:5, 133:11, 134:8, 140:18 turned 15:13, 105:18 two 14:8, 19:17, 19:22, 20:13, 26:19, 37:19, 42:14, 55:17, 56:10, 56:19, 56:22, 57:4, 77:14, 95:1, 96:15, 96:17, 99:12, 120:9, 125:4, 137:1, 137:12, 137:13, 141:14 twofish 97:8, 97:11, 97:13, 97:17 type 41:1, 47:14, 48:6, 49:20, 58:8, 58:9, 95:8, 98:16, 99:7, 99:14, 125:20, 131:14, 131:22, 134:2, 134:4, 136:7, 138:9 types 17:9, 43:19, 44:4, 45:8, 46:3, 46:13, 50:9, 50:14, 52:11, 72:22, 73:14, 78:20, 79:19, 91:6, 100:15, 138:1 typically 33:15, 64:10, 97:3 U ultimately 97:20 unattainable 34:9, 34:13,
---	--	--	--

34:21 under 26:9, 35:17, 35:19, 36:2, 40:19, 68:21, 119:15, 126:5, 129:20 understand 7:4, 7:8, 7:12, 18:11, 26:1, 26:4, 27:13, 28:14, 29:15, 60:18, 61:5, 62:17, 82:17, 83:4, 83:18, 88:16, 89:21, 102:14, 124:18, 128:7, 128:11, 132:12, 133:20 understanding 30:8, 35:17, 40:19, 52:3, 52:18, 53:8, 55:7, 55:8, 56:7, 62:1, 86:2, 86:10, 89:10, 94:22, 98:10, 98:15, 100:6, 101:7, 109:4, 118:4, 140:12, 141:8 understood 67:20, 74:10, 74:13, 85:18, 90:16, 96:8, 96:21, 141:13 undo 124:16 unique 125:7, 133:4 uniquely 57:8, 57:9, 95:3, 141:4 united 1:1, 4:16, 4:18, 4:20, 5:4, 5:7, 34:3 unkeyed 24:7	unless 25:3 until 13:3 uploaded 131:6 uploading 107:3 use 7:20, 24:7, 45:21, 53:4, 56:18, 75:19, 78:12, 91:12, 92:12, 97:4, 103:18, 104:8, 104:17, 104:19, 109:2, 131:8, 132:1 useful 34:2, 91:14, 96:5, 96:9 useless 110:16 user 23:6, 23:17, 27:6, 27:8, 27:22, 33:7 uses 56:15, 58:8, 58:9, 106:17, 132:8 using 56:22, 60:16, 81:11, 84:5, 84:15, 95:19, 98:10, 99:7, 99:14, 105:10, 124:15, 131:21, 140:9 usually 49:15 utilize 90:18 utilized 92:9 V value 37:20, 45:12,	45:15, 58:15 values 73:4, 134:18, 134:19, 134:21, 138:15 variation 80:9 variations 59:19, 80:18 various 13:8, 13:13, 39:10, 39:17, 58:17, 71:8, 93:22, 126:16 venable 3:4 version 133:5 versions 125:4 versus 78:13, 104:15, 134:5 via 2:2, 3:2, 3:9, 9:9 videoconference 2:2 videotaped 1:14 viewer 9:4 vigilytics 1:8 violate 85:21 violation 71:11, 117:7, 118:2, 118:7, 118:11, 122:4, 126:5 virtually 146:14 virus 28:21 vocabulary 93:10, 103:13, 103:18, 103:20,	104:2, 104:8, 104:14, 104:21, 105:6, 106:18, 107:21 vote 20:17 voter 20:15 W want 15:18, 19:21, 20:2, 20:16, 25:2, 38:2, 38:3, 48:1, 51:11, 60:9, 69:15, 71:12, 75:19, 76:5, 84:9, 102:19, 104:8, 108:9, 115:2 wanted 55:22, 67:16, 68:1, 68:8, 77:18, 78:15, 104:11, 108:16, 108:18, 122:19 warehouse 39:10, 93:18, 93:21, 94:3, 95:7, 95:10, 95:18, 95:20, 101:19, 101:21, 104:9, 107:3, 131:11, 131:15 washington 2:14, 3:6 way 6:12, 9:20, 19:3, 33:13, 33:19, 36:21, 38:12, 45:13, 45:19, 46:3, 53:4, 64:13, 64:16, 65:4, 78:22, 82:16, 86:4, 86:8, 94:9, 106:7,
---	---	--	--

118:5, 120:16, 121:19, 122:16, 123:20, 125:22, 128:5, 134:17, 137:8, 146:21 ways 29:15, 43:21, 60:12, 60:18, 61:15, 112:22, 113:14, 138:8 we'll 145:7 we're 117:2, 127:9 we've 39:19, 72:7, 105:6, 106:19, 115:10, 139:1 wednesday 145:3 week 145:3 weeks 36:9 well-known 37:14, 98:18 went 19:20, 130:3 whatever 24:9, 24:12, 29:15, 108:7, 108:10, 111:1 whenever 35:1 whereof 147:1 whereupon 39:21, 69:18, 72:9, 87:6, 115:13, 139:4, 139:16, 145:8 whether 22:13, 33:8, 36:11, 40:17, 41:5, 51:13, 55:11, 55:16, 56:11, 59:9, 70:4, 72:3,	116:19, 117:10, 118:6, 118:10, 118:15, 123:2, 123:4, 124:6, 127:15, 128:19, 128:21, 129:17 whole 48:10, 82:4, 82:19, 106:12, 116:7 whomever 29:2 widely 44:21 window 9:4, 105:15 within 38:8, 71:5, 79:22, 103:12, 107:5, 146:3 without 47:7, 55:12, 64:18, 72:4, 101:1, 101:15, 101:20, 102:1, 107:20, 108:19, 130:16 witness 4:6, 9:16, 69:6, 69:10, 69:13, 87:5, 139:11, 146:5, 146:9, 147:1 word 24:11 words 33:4, 106:17, 131:8 work 9:19, 12:19, 13:22, 20:20, 26:8, 33:10, 36:9, 44:14 worked 12:21, 19:15, 42:3, 42:5 working 12:17, 13:12,	14:4, 34:1 works 103:1 wouldn't 16:6, 22:5, 24:18, 32:3, 35:2, 35:5, 35:8, 55:12, 68:11, 70:12, 71:13, 94:12, 95:20, 103:4, 106:10, 117:5, 121:3, 121:10, 122:15, 123:20, 132:2, 143:13 wrong 82:11, 116:16, 127:1 wrote 15:18 Y yeah 27:12, 42:16, 72:2, 97:13, 105:14 Z zero 44:13 zeros 113:2 zip 68:6, 68:10, 73:3, 137:11 zoom 2:2, 3:2, 3:9, 9:4 0 00226 1:11, 10:2 0111833 5:6 0294111 4:22 1 10 4:17, 59:14,	61:17 1001 4:16, 10:6, 10:7 1005 4:18, 10:21, 11:1, 50:17 1006 4:20, 11:5, 11:7, 87:9 1007 5:4, 11:10, 11:13, 110:3 1008 5:7, 11:16, 11:19, 115:16 1009 5:9, 12:1, 12:3, 134:9 109 85:3 11 4:19, 4:22, 5:6, 5:8, 31:3, 32:16, 80:7, 133:11 118 86:19 119 108:20, 109:1, 109:16 12 5:9, 31:4, 51:17, 53:18, 62:10, 79:5, 85:8, 140:2, 140:4, 140:5, 140:20 12704567 147:11 128 44:11 13 54:21, 55:1, 56:14, 73:21, 83:9, 133:1, 140:2, 140:5, 140:18, 140:20
---	--	--	--

Transcript of Aviel D. Rubin, Ph.D.
Conducted on November 22, 2024

182

138 39:11 139 4:8 14 74:19, 83:22, 131:1, 141:19 141 103:9, 103:12, 105:1 143 81:1 144 4:9 146 4:11 147 1:21 15 82:10, 82:12, 89:2, 139:13 16 66:3, 67:5, 85:8, 97:16 170 129:6 171 118:18, 118:19, 129:7 18 16:17, 16:20, 68:4, 132:6, 147:4 19 55:2 1991 43:20, 46:1, 47:11 1s 113:3 2 2 145:9, 146:15 20 55:2, 63:1, 85:8 20001 3:6	2001 5:10 2002 5:6, 5:9, 17:6 2003 12:22, 17:6 2007 4:22 2009 14:1, 41:15, 41:19, 41:22, 42:3, 42:7, 111:18 2011 12:18, 12:20, 13:3 202 3:7 2021 9:18, 10:4 2024 1:11, 1:16, 10:2, 146:15, 147:3 2028 147:4 22 1:16, 21:6, 146:15 24 79:6, 114:2, 114:4 26 131:2 27 93:13, 93:16, 94:6, 147:2 29 61:18 3 30 72:12, 102:3 31 32:17 312 23:20, 25:15, 25:17, 26:2,	26:5, 27:5, 27:21 318 25:15, 25:18, 25:19, 26:2, 26:5, 39:2 32 1:17, 63:22, 145:9, 146:15 320 39:3 3200 3:15 33 73:22, 74:2, 83:10 335 3:17 344 3:7 35 83:13 36 53:18 37 59:15 38 94:15, 95:2, 96:1, 115:19 39 50:20, 50:22 4 4000 3:7 41 73:6, 96:14, 97:7, 97:22, 98:7, 98:8, 117:17, 117:20 43 74:3, 80:8 45 44:13, 110:5, 110:8, 110:12, 110:13, 112:3, 112:19 46 113:7, 113:21	47 60:3, 77:22, 115:21, 142:15 48 62:11, 89:14, 142:15 49 57:16, 57:18, 67:5 5 50 99:19 5070 3:17 51 101:12 52 126:10, 127:11, 133:12 53 57:18, 117:20 552 134:11, 135:3 554 136:8 55402 3:16 555 136:13 556 137:17, 138:11 56 85:6 562444 1:20 58 20:22, 21:2, 21:5, 22:18, 30:18 6 6- 147:4 60 3:14, 34:5, 36:14, 37:8, 104:1, 105:2
---	--	--	---

600 3:5 61 38:14 612 3:17 63 51:18, 66:4 641 8:21, 10:9, 10:15, 22:20, 30:11, 35:3, 35:9, 38:8, 48:9, 48:18, 109:21 66 105:12, 105:20, 106:19, 107:11 6th 3:14 7 7,519,591 5:8 7,823,207 4:19 73 107:16 74 40:1, 40:4 78 103:12 8 8 1:17, 146:15 80 9:14 802 147:8 9 9,118,641 1:12, 4:17, 10:12 90 25:1 95 118:18		
---	--	--