UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,

Petitioner,

CERTIFIED COPY

v.

VIGILYTICS LLC,

Patent Owner.

Case 2024-00226 (US Patent No. 9,118,641)
Ref. 25412-0020IP1
Proceeding No. IPR2024-00226

VIDEOCONFERENCE DEPOSITION OF

DR. PAUL CLARK

September 26, 2024

Page 1 - 101 9:38 a.m. - 2:08 p.m. EST

REPORTED BY:
Tamara L. Houston
CA CSR No. 7244, RPR, CCRR No. 140
Job Number 142600

Exhibit 2008
Datavant v. Vigilytics
IPR2024-00311

REMOTE VIDEOCONFERENCE DEPOSITION OF DR. PAUL CLARK, taken on behalf of the Patent Owner, commencing from 9:38 a.m. to 2:08 p.m. EST, Thursday, September 26, 2024, before Tamara L. Houston, CSR No. 7244, CCRR, RPR.

APPEARANCE OF COUNSEL:

On behalf of the Petitioner:

VENABLE LLP
BY: JUSTIN J. OLIVER, ESQ.
600 Massachusetts Avenue, NW
Washington, DC 20001
(202) 721-5423
joliver@venable.com

On behalf of the Patent Owner and Witness:

FISH & RICHARDSON, P.C.
BY: NICHOLAS STEPHENS, ESQ.
RISHA GUPTA, ESQ.
JEFFREY BARCLAYM, ESQ.
INDRANIL SARKER, ESQ.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, Minnesota 55402
(612) 335-5070

INDEX TO EXAMINATION

WITNESS: DR. PAUL CLARK

EXAMINATIONS PAGE

Mr. Stephens..... 6

QUESTIONS INSTRUCTED NOT TO ANSWER

Page Line

NONE

INDEX TO EXHIBITS

DR. PAUL CLARK

DATAVANT, INC. vs. VIGILYTICS LLC

September 26, 2024

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

EXHIBIT	DESCRIPTION	PAGE

--o0o--

(Exhibits marked electronically.)

Thursday, September 26, 2024, 9:38 a.m.

--o0o--

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

EXAMINATION BY MR. STEPHENS:

Q. Good morning, Dr. Clark.

A. Morning.

Q. My name is Nick Stephens. I'm an attorney with Fish & Richardson. I'll be taking the deposition today on behalf of the patent owner, Vigilytics LLC.

I'm joined by my colleagues Indranil Sarkar, Rishi Gupta, and Jeffrey Barclay, each with Fish & Richardson.

Would counsel for Petitioner like to make your appearance?

MR. OLIVER: Justin Oliver of Venable on behalf of the Petitioner, Datavant.

BY MR. STEPHENS:

Q. We're here today regarding inter partes review proceeding IPR 2024-00226 involving U.S. patent 9118641.

Do you understand, Dr. Clark?

A. Yes.
Q. You understand that this deposition is being transcribed, correct?
A. Yes.
Q. To ensure a clean record, I'll aim not to interrupt you while you're speaking and answering my questions.
Will you be able to do the same for me?
A. I think so, yes.
Q. If you need a break at any time, just let me know. In general, I'll aim to break about every hour, and we can take a lunch break as needed later in the day. Okay?
A. Yeah. It's up to you. I don't need breaks, but whenever you want one, take one.
Q. Sure. If you happen to need one, just let me know.
And you indicated before we went on the record that you'd received our binder with electronic copies of documents from the record in the IPR, correct?
A. Yes. I put those in the dedicated folder for the duration of this dep.
Q. Do you have any other copies of documents with you?
A. No. As I said, it's a dedicated window. I

shut down those.

Q. Okay. Are you in communication with anyone at this time outside of the dedicated window?

A. No, sir.

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

A. Paul Christopher Clark.

Q. And please state your city of residence.

A. Bethesda, Maryland.

Q. You understand that you are under oath today?

A. I do.

Q. Is there any reason that you cannot give truthful and accurate testimony today?

A. No.

Q. For clarity, I'll define several terms that will be used throughout the questioning today. When I use the terms "Petitioner" or "Datavant," I am referring to Datavant, Inc.

Do you understand?

A. Yes.

Q. And when I use the terms "patent owner" or "Vigilytics," I'm referring to Vigilytics LLC.

Do you understand?

A. Yes.

Q. When I use the term "'641 patent," I'm

referring to the patent that's been marked as Exhibit 1001 in this proceeding. That's U.S. patent 9118641.

Do you understand?

A. I do.

Q. When I use the phrase "this IPR" or "this proceeding," I'm referring to the inter partes review proceeding, IPR 2024-00226.

Do you understand?

A. Yes.

Q. When I use the acronym POSITA or POSA, I'm referring to a person of ordinary skill in the art at the time of the alleged invention.

Do you understand?

A. I do.

Q. I also might refer to a number of exhibits through the course of the deposition. I'd just like to index them for the record.

When I'm referring to "your declaration" or "the declaration," I refer to -- I'm referring to Exhibit 1003 in this proceeding.

Do you understand?

A. Yeah. They are labeled as such in the folder you provided.

Q. Great.

When I refer to "Evenhaim," I'm referring to Exhibit 1005.

Do you understand?

A. As I said, yes.

Q. And when I refer to "Settimi," I am referring to Exhibit 1006.

Do you understand?

A. That's how it's labeled.

Q. When I refer to "Dick," I'm referring to Exhibit 1007.

Do you understand?

A. That's the way it's labeled. As I said, all of them are labeled that way.

Q. Almost done here.

And when I refer to "Murphy," I'm referring to Exhibit 1009.

Do you understand?

A. As labeled, yes.

Q. Can you please describe how you prepared for today's deposition?

A. I had a meeting with counsel over the course of two days, and prior to that, I had reread the references in my declaration.

Q. Did those meetings occur this week?

A. Yes.

Q. Approximately how much time did you spend preparing for the deposition?

A. I don't know. Maybe 20 hours; maybe less.

Q. What documents did you review in preparation for your deposition?

A. As I said, the references in my declaration primarily.

Q. Is there any material that's not identified in your declaration that you reviewed for today's deposition?

A. Maybe, but not that I recall sitting here.

Q. Before this IPR, have you ever served as an expert in any capacity for Datavant?

A. Not that I recall. It's not impossible, but not that I recall.

Q. Have you ever done any consulting for Datavant before this IPR?

A. No.

Q. Have you ever collaborated on research projects with Datavant?

A. No.

Q. And have you ever worked with Datavant's counsel before Venable?

A. Yes. I've worked with Venable, but not with this particular attorney.

Q. In what capacity did you work with Venable?
A. As an expert.
Q. Do you recall if those matters were IPRs?
A. I do not. I don't think they were, but, again, it's not impossible. I haven't worked with them recently.
Q. Can you please describe the process by which you prepared your declaration in this proceeding?
A. I reviewed the patent, file history, various other documents. Went through references that I had, looked at references that were provided to me, and then put together, in a collaborative effort, the declaration that's in front of you.
Q. Can you describe the nature of that collaborative effort in preparing the declaration?
A. Like any expert you work with, just -- I provided my opinions, and I wrote some stuff, and they wrote some stuff. And you end up with a declaration.
Q. There are portions of the declarations that were written by counsel rather than by you?
A. As I said, it's a collaborative effort, but I'm certainly responsible for the contents of the declaration.
Q. Approximately what percentage of the declaration was drafted by counsel?

A. I don't know.
Q. You don't recall?
A. Nope.
Q. If you had to put your best estimate on it, how much do you believe was drafted by counsel?
A. I don't have an estimate for you. I'm not going to guess.
Q. Approximately when did you begin working on your declaration?
A. Several months ago.
Q. Is there a timeframe that you're able to provide?
A. Not from memory, no.
Q. Apart from counsel, did you have anyone, such as an assistant, help you with your declaration?
A. No.
Q. On page 7 of the declaration -- that's Exhibit 1003 -- you provided a list of documents that you indicated had been considered in forming your opinions in the declaration, correct?
A. That's what it says, yes.
Q. Were there any other documents that are not identified in this table that you considered in forming your opinions?
A. My experience. All the documents that I've

read in this field all make up my background. So, yes, I'm sure there's a whole bunch of them.

Q. Were there any specific documents that you recall reviewing while preparing this declaration?

A. I see the Kerberos one that you provided. That one came to mind immediately.

Q. Do you currently have any opinions regarding the '641 patent that are not contained in your declaration?

A. Not -- not that I'm aware of. I'm sure we're going to explore that, though.

Q. Have any of your opinions that are stated in the declaration changed since the time that you submitted the declaration?

A. Not that I'm aware.

Q. And are you currently aware of any errors that exist in your declaration?

A. Not that I'm aware.

Q. Similarly, are you aware of any typos in your declaration?

A. I didn't read it necessarily for typos, but any that I caught, I would have remedied.

Q. In your career, approximately how many times have you been retained as an expert in litigation matters?

A. Going back to 1995, probably 25 times. I don't know. I think you have the case list for the last five or ten years.

Q. Would you say more than two dozen times?

A. No. More than 25 times.

Q. More than 25 times.

And do you know approximately how many IPRs you've been involved with?

A. Maybe ten. Probably a few more than that.

Q. You've been deposed in the past, correct?

A. Yes.

Q. Approximately how many times have you been deposed?

A. A couple of dozen, probably.

Q. In your declaration at paragraph 2, you indicated that you're being compensated for your time at your normal consulting rate of 590 an hour?

A. That's correct.

Q. And is that still the case, you're being compensated at that rate?

A. Yes.

Q. Is your compensation for your work on this case in any way contingent on any factor other than the number of hours in which you work on the case?

A. Of course not.

(Court reporter requested clarification.)
BY MR. STEPHENS:
Q. To your knowledge, has a Court ever precluded you from offering an opinion?
A. No.
Q. To your knowledge, has a Court ever criticized your opinions?
A. No.
Q. And, to your knowledge, has a Court ever excluded your opinions?
A. No.
Q. All right. In the package that I sent, I included Exhibit 1004, which is a copy of your curriculum vitae.
Just let me know when you have that available.
A. I just brought it up.
Q. So I understand that you are the president and CTO currently of SecureMethods Inc./Paul C. Clark LLC. Is that correct?
A. That's correct.
Q. And you've held these positions since July 1999?
A. Yes.
Q. And what are your responsibilities in these roles?

A. I basically run the company. It's a sole prop LLC currently, and so I'm responsible for day-to-day operations.

Q. Do you -- have you worked with other companies -- I'm sorry.

Have you been employed by other companies during this timeframe?

A. Yes, I'm the CEO of Clear Guide Medical for the last six or seven years.

Q. And that's not identified on the CV, correct?

A. It's not relevant.

Q. What does your work at Clear Guide Medical involve?

A. I'm the CEO, and we do AI-guided medical procedures. We have a suite of products that address that issue.

Q. Can you elaborate a little bit on that work, what the AI entails?

A. Yeah. You do instrument recognition and targeting and use the computer to guide the clinician onto the target with whatever the instrument is.

Q. Apart from Clear Guide Medical, are there any other companies that you're employed by?

A. Not as an employee, no.

Q. And from January 1995 to July 1999, I

understand that you were the chief scientist at DynCorp network solutions. Is that correct?

A. That's correct.

Q. What were your responsibilities in that role?

A. I was essentially the chief technical person for that division of DynCorp.

Q. Did your -- can you describe the nature of the projects that you worked on at DynCorp?

A. Yeah. They were security-related projects for primarily government and DOD customers, some commercial.

Q. At DynCorp, were you ever involved in the design or implementation of a HIPPA-compliant medical record system?

A. Well, this was while HIPAA was being developed, so I was involved with the policy people, and we did secure databases. So, yes, we did data filtering and de-identification of sensitive data. So the answer is yes.

Specifically for medical, we had some work with a healthcare client that involved, again, controlling access to PII, so the answer would be yes.

Q. And was that specifically in relation to your work at DynCorp?

A. Yes.

Q. Have you been involved in the design or

implementation of a HIPAA-compliant medical record system at any other point during your -- during your career?

A. At -- SecureMethods had a healthcare client that was concerned with protecting PII, so from a technical perspective, yes.

Q. Who is SecureMethods?

A. SecureMethods is my company. I founded it.

Q. I'm sorry.

You said SecureMethods had a healthcare client that was concerned with protecting PII?

A. Yes.

Q. And so in your work with that client, were you involved with ensuring compliance with the HIPAA privacy rule?

A. Not the policy aspects; the technical aspects. So the answer is we did the de-identification and the data security to be compliant with HIPAA, but we were not the ones that evaluated it.

I think there's also -- in my publication list, you'll find a paper that was published -- I think dealing with HIPAA compliance again from a technical perspective.

Q. Do you see that in the list in your CV?

A. Let me see if it's there.

No, it's not there. It was for a minor conference. These other ones were larger publications.

Q. Would you have been a named author on that paper?

A. Yes.

Q. Were there any co-authors that you recall on the paper?

A. Yes. Probably the same ones listed on the ACSAC paper that is on my CV.

Q. And do you have an understanding of what the HIPAA privacy rule is?

A. Yes.

Q. Can you describe your understanding of the HIPAA privacy rule?

A. That it guarantees individuals control over access to their medical records and, to the extent they haven't provided authorization, the PII must be de-identified before it can be disseminated.

Q. And do you understand what covered entity is under HIPAA?

A. I don't have a specific definition. But, yes, I mean, I know what a covered entity is.

Q. In general, what's your understanding of a covered entity?

A. The entities that are subject to the HIPAA

regulations.
Q. The entities that must comply with HIPAA?
A. Correct.
Q. What types of entities may be deemed covered entities under HIPAA, in your experience?
A. Well, the guys with the money are the insurance companies, obviously. They have the biggest stake in it. But also research institutions, big pharma all have an interest in being able to do data mining.
Q. If I use the term "covered entity" during my questioning today, will you understand what I'm referring to?
A. Yes.
Q. All right. Let's turn to paragraph 26 of your declaration, please.
A. Which paragraph again, sorry?
Q. Paragraph 26.
A. I'm there.
Q. And this starts a section in your declaration related to claim construction; is that correct?
A. Yes.
Q. You state that, "I applied the term's ordinary and customary meaning in accordance with my understanding of how a POSA would understand them in July of 2009," correct?

A. That's what it says.
Q. And then in paragraph 28, you indicated that, with respect to certain terms, you'd adopted patent owners' claim constructions from a litigation involving the '641 patent in Massachusetts; is that correct?
A. Yep. That's what it says.
Q. These terms include "token," "server," "similarly encrypted," and "medical information" that characterizes the group, correct?
A. Yes.
Q. And based on your review of these terms, do you agree that they are the correct constructions?
A. No. They are just the ones that I use. I mean, you apply the constructions that the Court or the attorneys or whatever analyses you need to provide is, and my agreement or disagreement doesn't matter.
Q. Have you formed an opinion as to whether you agree or disagree with these constructions?
A. No, but I just apply them.
Q. Did counsel for the Petitioner ask you to apply these constructions?
A. Yes.
Q. Just like to go through these individually.
The construction that you adopted for token was "an identifier associated with an individual that

does not reveal the identity of the individual," correct?

A. That's what it says.

Q. Do you have any reason to believe that that construction is incorrect?

A. Again, it doesn't matter. I don't have an opinion on whether they are correct or not. I simply apply them.

Q. You reviewed the specification and file history of the '641 patent, correct?

A. That is correct.

Q. Is the construction that's provided in your declaration for a token consistent with the use of token in the '641 patent?

A. I mean, I think so. Again, I haven't done that analysis. I haven't seen anything that directly contradicts it.

Q. And as to a server, you adopted the construction of a computer with a processor and memory on a network that provides information in response to requests from another computer, correct?

A. That's what I used.

Q. Is this construction consistent with your understanding of the term "server" in the '641 patent?

A. As I said, I haven't seen anything to

contradict that. I mean, it might be slightly broader, but it doesn't matter.

Q. And then as to similarly encrypted, the adopted construction is, "Generated such that tokens generated from corresponding information can be compared to one another to detect a match," correct?

A. Yes.

Q. Based on your review of the '641 patent, is this construction consistent with the specification and file history of the patent?

A. Again, I haven't seen anything that contradicts that. And in order for the systems to work, it would need to work that way.

Q. And then similarly with respect to medical information that characterizes a group, is the adopted construction consistent with your understanding of that term from review of the '641 specification and file history?

A. Well, it's plain and ordinary meaning, so I would assume that to be consistent.

Q. And then in the final bullet under paragraph 28, you indicated that, "A POSA would understand the foregoing construction of token to encompass encrypted identifying information, which is stated by the '641 patent," correct?

A. Yeah, that's one of the ways you could create a token.

Q. And what prompted you to add this clarification as to the meaning of token?

A. I was probably asked the question by the attorneys.

Q. I'll refer to Claim 1 of the '641 patent, Exhibit 1001.

A. Okay. I'm there.

Q. And under the producing step -- do you see, at line 30, "producing"?

A. Yes.

Q. And the claim language recites, "Producing, by processor of an encryption server, tokens wherein the identity of the individuals in the group is unattainable from the tokens," correct?

A. Yes.

Q. What does it mean, in your view, for the identity of the individuals in the group to be unattainable from the tokens?

A. Computationally infeasible to attain.

Q. Can you elaborate? What does computationally infeasible mean?

A. It means it would take a computer too long to figure it out.

Q. So would a hash -- would a one-way hash be an example of a token?

A. Depends on the hash. But, I mean, that's a one-way encryption.

Q. And what would -- what factors would you consider to know if the hash -- whether the identity of the individuals in the group would be unattainable from a hash?

A. Whether it was computationally infeasible to derive them.

Q. Does that mean computationally infeasible to recover the original value that was hashed?

A. Without keying in -- or additional information, yes.

Q. Are there any other factors that you would consider to know whether the identity of individuals in the group is unattainable from the tokens?

A. That's a pretty broad question. But within the scope of the patent where we're talking about encrypted information, I would understand that unattainable to be cryptographically unattainable, which means computationally infeasible to brute force.

Q. Okay. Let's turn to Exhibit 1005. Evenhaim.

A. Okay.

Q. You're familiar with the Evenhaim records,

correct?

A. Yes.

Q. Did you review Evenhaim while preparing your declaration in this proceeding?

A. Yes.

Q. And have you read Evenhaim in its entirety?

A. Yes.

Q. How did you first encounter the Evenhaim reference?

A. It was provided to me.

Q. Do you recall if you were aware of Evenhaim before your involvement in this IPR?

A. I don't recall. I've been involved in a couple of other de-identification matters, so it's possible that I've seen it.

Q. Do you believe you have a good understanding of the technology described in Evenhaim?

A. Yes.

Q. Is there any reason that you would not be able to explain the technology described in Evenhaim in response to my questions?

A. No, but we'll find out.

Q. All right. Let's turn to figures 4 -- I'm sorry. Figures 4 and 4A of Evenhaim.

A. Okay.

Q. Just let me know when you're there.
A. I am.
Q. And Figure 4 shows representations of computing systems operated by a pharmaceutical company, Crossix, and health plan/pharmacy benefit managers, correct?
A. Yes.
Q. Figure 4A then shows representations of computing systems operated by a data consumer entity, a data aggregator, and data source entities, correct?
MR. OLIVER: Objection. Form.
THE WITNESS: I mean, I see those things in 4B, yes. Or 4A, sorry.
BY MR. STEPHENS:
Q. Do you understand the health plan or PBM entity shown in Figure 4 to be examples of data source entities?
A. I mean, they could be. They could also be consumers.
Q. Are they -- are they described in Evenhaim as consumers?
A. I don't have complete recollection. Evenhaim describes lots of different embodiments.
Q. What is a data source entity in Evenhaim?
A. An example of such an entity might be a

doctor's office or hospital or something like that.

Q. And data source entities can maintain identifiable patient-level microdata?

A. They can.

Q. A data source entity would be responsible for complying with HIPAA, correct?

A. Yes, they have to protect the PII.

Q. So they would be covered entities under HIPAA?

A. That would be my understanding.

Q. And then why is it important that the data source entities not release private medical information of individuals without their authorization?

A. That's what the law tells them to do.

Q. Would you agree that the pharmaceutical company depicted in Figure 4 is an example of a data consumer entity?

A. You're talking about the pharmaceutical entity?

Q. On the left-hand side, that's right. Pharmaceutical company.

A. Yes. I mean, again, they may come into possession of PII as well. But in this example, they're one of the consumers.

Q. And what is a data consumer entity in Evenhaim?

A. It's somebody who is attempting to search the patient data.

Q. And a data consumer entity is not necessarily a covered entity under HIPAA, correct?

A. To the extent they don't have -- to the extent they don't have access to PII, they are not.

Q. In Figure 4, the Crossix system shown in the center of the figure is an example of a data aggregator in Evenhaim, correct?

A. Yes.

Q. What is a data aggregator?

A. It's functionally a database server, DDMS, that also includes encryption and token matching capabilities.

Q. And the data aggregator is not necessarily the covered entity under HIPAA, correct?

MR. OLIVER: Objection. Form.

THE WITNESS: No, it could be. I mean, if it has access to the PII -- again, it depends on how the databases are architected. But if it -- if it has access to the PII, it's covered.

BY MR. STEPHENS:

Q. Are you aware of any disclosure in Evenhaim where the data aggregator has access to PII?

A. I don't have complete recollection, but I

believe that it's constructing tokens in some of the embodiments. So, yes, it would need access to the PII in order to access or create those tokens.

Q. Are you aware of any disclosure in Evenhaim where the data aggregator has access to PII correlated with that individual's medical data?

A. Yes. I mean, one of the examples, they're encrypting, you know, patient lists, like I see in Number 3. And that's certainly PII.

Q. And in that example, the patient lists don't contain the patients' medical data, correct?

A. They may or may not have access to the data. Again, Evenhaim provides lots of possibilities.

Q. Is there -- are you able to identify any disclosure in Evenhaim where the patient lists would have -- would include medical data of the patients on the list?

A. I -- I would have to read the entire reference. I'll do so if you wish, but I know that one of skill in the art would understand that one possible implementation of this would have the Crossix server accessing PII.

Q. I'd invite you to review the specification and let me know if you see any examples where the data aggregator does have a patient list that includes the

patients' medical data.

A. At least in Figure 5, it says, (as read) "Analyze all patient records on the patient ID list," so that would include the medical data from my perspective.

Q. And in Figure 5, that's a box shown within the data cruncher module, correct?

A. Yes.

Q. And the data cruncher module is part of the data source entity rather than the data aggregator, correct?

A. I think it could be implemented either place. Again, it depends on how the database is architected. This reflects one embodiment, but you could certainly put it anywhere.

Q. Are you able to identify any disclosure in Evenhaim where the data cruncher module is located at the data aggregator?

A. Well, it -- again, Evenhaim provides several embodiments, some of which have PII processing on the aggregator and some of them which don't.

Q. So there's no disclosure of the data cruncher module being part of the data aggregator, correct?

A. It would -- those functions would necessarily need to occur on the aggregator, depending upon the architecture of the database. Evenhaim is just telling

you the things that need to happen and potential places where they could happen.

Q. But there's no basis for -- in Evenhaim itself in which it's disclosed that the data cruncher module is located on the data aggregator, correct?

A. No, that's not correct.

Q. Are you able to identify a disclosure where the data cruncher module is located on the data aggregator?

A. We can find a disclosure of an embodiment in which the PII is on the aggregator, in which case the data cruncher functions would have to be performed there, as I've explained.

Q. You said that "we can find," but I'm waiting for it to be found.

Is there an example that you can point me to?

A. Is there an -- you want me to go through and find where PII is processed on the data aggregator? We've already done that.

Q. Where the data cruncher module is located on the data aggregator.

A. I'm not --

Q. Why don't you -- we don't -- if you're not able to point to any disclosure, that's fine. We can move on. I'm just -- I'd like to be sure for the

record.

A. Well, for the record -- which I'm explaining to you. I understand what you're trying to do.

But for the record, the figures are particular embodiments. And so the disclosure, the written text, talks about the processing of PII on the aggregator, and that would necessarily require those cruncher functions, in whole or in part, to be on that aggregator by the disclosure in text. They are not shown in the figures.

Q. I appreciate your position, Dr. Clark.

I'm looking for any specific examples in Evenhaim where the data aggregator has PII along with the patient's medical data.

Are you able to identify any specific examples?

A. And you want that to be on the aggregator?

Q. On the aggregator, correct.

A. All right. So sit back and relax.

Well, we can start with the abstract. Says, "Between a secure aggregator" -- and it needs to be secure if it has PII -- "and" -- conjunctive -- "sources having respective access to privacy-sensitive microdata."

So in that case, the PII is on the aggregator.

Q. And are there any examples of the patient list

processed by the aggregator, including medical data?

A. It says --

MR. STEPHENS: Object to form.

THE WITNESS: It says, "Privacy-sensitive microdata." I understand that to include PII and medical data. I mean, that's the subject of the reference.

BY MR. STEPHENS:

Q. And what is your understanding of what the data aggregator does with the patient list?

A. It depends on the particular embodiment. In general, it's gonna use it to facilitate the searching of the sensitive data.

Q. So it would send the patient list to the data source entities; is that correct?

A. That's one way it could do it.

Q. Are there other ways that you have in mind that it can do it?

A. Yes. As I said, it can create the tokens and search for tokens in the database. It has -- it has to be secured because it has access to the PII.

Q. Let's turn back to Figure 4.

And there are a series of steps shown in this figure, 1 through 7, correct?

A. Yes.

Q. Can you describe your understanding of what happens at each of these steps?

A. This is one particular embodiment. Is there any in particular that you're interested in, or you want me to talk through all of them?

Q. In the embodiment that's shown in Figure 4.

A. All right. So you have a pharmaceutical company attempting to access covered entities using the Crossix server, and so it sends a request using the user interface provided by the Crossix server.

And the Crossix server generates the query to one or more databases and then aggregates the results -- makes sure, presumably, that they don't have PII in them -- and then sends it back for final analysis to the requester.

Q. And so in the operations shown in Figure 4, we have data being transmitted between the data aggregator and the data source entities, correct?

A. Well, yes, they're the -- they have the patient-level microdata, as it says.

Q. And this data could be transmitted over communication networks, correct?

A. It depends on the particular implementation. You would seek not to let that PII escape past your security boundary.

Q. What do you mean by "security boundary"?
A. Well, the Crossix server is the security boundary between the requester, to the extent they are not sending PII back, and the sensitive data.
Q. The requester, is that a pharmaceutical company in Figure 4?
A. Yes.
Q. At Column 13 of Evenhaim at lines 33 to 36, Evenhaim discloses that, "Every step requiring a transmitting of data (or of at least one file) and every respective associated step requiring receiving of that data (or of that at least one file) may preferably include respective encryption and decryption."
Did I read that correctly?
A. That's what it says.
Q. And further down that paragraph, Evenhaim discloses that it's "generally preferable to include some degree of data transmission security," correct?
A. That's what it says.
Q. Do you have an understanding of data transmission security?
A. Sure.
Q. What is data transmission security?
A. You're going to prevent unauthorized disclosure, integrity violations, those sorts of things.

Q. What do you mean by "unauthorized disclosure" and "integrity violations"?

A. Those are terms of art. I mean, you don't want the data modified, and you don't want unauthorized people seeing the data.

Q. And so encryption would be one way to provide data transmission security?

A. Encryption will prevent unauthorized disclosure.

Q. And with regard to data integrity, what can you do to provide data transmission security?

A. Hashes are one way to do that. Keyed hashes or message authentication codes are another way to do that. There are entire books on ways to implement those schemes.

Q. Are you familiar with any data transmission security schemes from the early 2000s?

A. Sure. Endless numbers. SSL being one to provide streaming-level security. There's also -- were protocols like S-HTTP, S/MIME, all sorts of ways.

Q. Have any of those ever been applied in Evenhaim to provide the data transmission security?

A. I'm sure they were used -- intent on using standard algorithms. It looks like they had their own protocol, however. They may have used that in

conjunction with other countermeasures, like I said, SSL, that existed to protect maybe the queries that were coming across.

Q. How is a message typically encrypted for data transmission security?

A. It depends on the implementation. As I said, there are any number of ways to do it.

Q. Are there -- would you typically need an encryption key for an encryption scheme?

A. If you're going to encrypt something, there's a protocol that needs to go with that that includes an algorithm, key management, all sorts of things.

Q. And can you just briefly describe. What is an encryption key?

A. It is a string of bits that's fed into an algorithm along with the data stream to produce a cipher text.

Q. And if you're encrypting a message for transmission over a network, do you encrypt the entire message at a time?

A. Not necessarily. It depends. I mean, some systems will actually use some form of super encryption where you have multiple layers of encryption. So, again, it depends on the implementation.

Q. If -- I guess, for super encryption, does that

mean you apply first kind of encryption to the message and then re-encrypt it?

A. It would mean that interior portions of the data are encrypted in addition to what you're focused on, which is streaming, like SSL-level encryption. Those are not incompatible.

Q. At Column 14, lines 3 to 4, Evenhaim notes that he's "returning to the abovementioned aspects of preferable encryption."

Do you see that?

A. Yes.

Q. And so that refers, again, to the description that we just went over in Column 13 about it being preferable to include some degree of data communication security, correct?

MR. OLIVER: Objection. Assumes facts.

(Court reporter requested clarification.)

THE WITNESS: Yeah. I mean, as I said, there's any number of encryption schemes available to protect data in different ways and at different levels of security.

So as I said, you can secure the channel and secure specific fields or items of data that you need to secure. And, again, that's dictated by policy. One of skill in the art would know that all of these were

available.

BY MR. STEPHENS:

Q. These are all schemes that would apply for data transmission security, correct?

A. Well, you're going to provide data security, and then if you choose to send it over a network, that may require something else. So that -- there's not a one size fits all.

Q. Can you elaborate on that? It requires security, and then if you send it over a network, that requires something else. Are there two different things there?

A. Sure.

I may secure the data on my server in various ways, including encryption, de-identification. And then I may also secure the channel once that data is being sent over the network so that I can protect, for instance, the contents of the query as well as the results.

And so it's quite possible to have a situation in which super encryption is occurring.

Q. In that paragraph at Column 14 at lines 4 to 7, Evenhaim notes that it's "certainly strongly advised that, regardless of the general level of encryption elected, a parameter list including 'individuals' should

carry a stronger level of encryption," correct?

A. That's what it says.

Q. Why would a stronger level of encryption apply to a parameter list that includes individuals?

A. As I said, you may wish to encrypt things one or more times or with different keys depending upon the level of protection you wish to provide. One -- anyone implementing one of these systems would know that.

Q. All right. Let's look back at Figure 4, if you would.

A. Okay.

Q. At Step 3 in Figure 4, the Crossix system is set to encrypt patient list and query, correct?

A. That's what it says.

Q. Do you agree that the query is encrypted at Step 3 to provide data transmission security?

A. Maybe; maybe not.

Q. Do you have an opinion?

A. Yeah, maybe or maybe not. It depends. I mean, this is a schematic of one embodiment. So, I mean, the motivation for encrypting that could be any number of things.

Q. In light of the disclosure that we read at Column 13 that it's generally preferable to provide data transmission security, would a person of skill in the

art reading Figure 4 understand that the query is encrypted to provide data transmission security?

A. No, not necessarily. The query could be encrypted because that's how it's going to match fields in the database. I mean, it depends on how the system is designed.

Q. And I'm not asking about the patient list right now. I'm asking about the query specifically.

So it's my understanding that the query does not include fields that would be matched in the database. Is that correct?

A. No. The query may very well include fields that would be matched.

Q. Is there a portion of Evenhaim that you are referring to for your understanding of the query?

A. The query is a term of art that refers to a database query. The standard for database queries is called SQL, and it includes things like "select from where," where "where" is your conditions and your query.

And if you need to match those, then it's possible that you would need to encrypt them in order to match them.

Q. What is a patient list as referred to in Step 3 of Figure 4?

A. I would understand it to be a list of patients

and identifiers.

Q. Is it possible that the patient list is encrypted to provide data transmission security in Evenhaim?

A. Anything is possible. I mean, that's why Evenhaim has so much disclosure.

Q. There is nothing that contradicts that understanding in Evenhaim?

A. There's -- no, there's certainly -- at least one of the embodiments would function that way.

Q. Let's look at Figure 5, please.

A. Okay.

Q. And within the data cruncher module, towards the top right of that module, there's a box that says, "Decrypt patient identifier list HP(i,j)."

Do you see that?

A. I do.

Q. Would you agree that, in Figure 5, each patient identifier list is decrypted separately from the other lists?

MR. OLIVER: Objection. Form. Foundation.

THE WITNESS: Yeah. I'm not sure I read that much into it. I take it at face value. It says, (as read) "Decrypt the patient identifier list."

That's a pretty broad function.

BY MR. STEPHENS:

Q. There are multiple patient identifier lists referenced in Figure 5, correct?

A. I mean, it does use plural. It allows for one or more patient lists, so I'm sure.

Q. What is your understanding of HP(i,j)?

A. It's a patient identifier.

Q. HP(i,j), that's referring to patient identifiers?

A. It is a particular patient identifier.

MR. STEPHENS: All right. We've been going for a bit over an hour. Would you like to take a -- I would actually appreciate it. Could we take a five-minute break?

THE WITNESS: Yes, that's fine. Let's make it a little bit longer, but, yes.

MR. STEPHENS: Ten minutes?

THE WITNESS: Fine.

MR. STEPHENS: Okay. Thanks.

(Recess: 10:50 a.m. to 11:04 a.m.)

BY MR. STEPHENS:

Q. Dr. Clark, during our break, did you discuss the substance of your testimony at all with counsel?

A. I didn't discuss it with anyone.

Q. Let's turn to Column 12, please, of Evenhaim.

Let me know when you're there.
A. I'm there.
Q. And in the paragraph that begins with "a further class of embodiments," Evenhaim refers to "interim data merger enabled embodiments," correct?
A. Yes.
Q. And then at line -- starting at line 12, Evenhaim discloses, "If the data sources are careful to encrypt the identifying portions of each record using a common encryption 'key,' then further down the data processing circuit, it will be possible to link records related to a common individual without compromising the identity of that individual."
Did I read that correctly?
A. What it says.
Q. The mention of data sources at line 13 can refer to the data source entities, correct?
A. I think it could, sure.
Q. Would you understand that multiple data sources can produce the same encrypted identifier for an individual by using a common encryption key?
A. That's not necessarily the way that I would implement it. But, I mean, that's what it says for this embodiment.
Q. And in this embodiment, the data aggregator is

the entity that would be further down the data processing circuit, correct?

MR. OLIVER: Objection. Form.

THE WITNESS: That would be one place you could do it. As I said, the functions could be anywhere on that side of the security boundary.

BY MR. STEPHENS:

Q. And so the data aggregator can link records related to a common individual, correct?

A. Using encrypted identifiers, yes. I mean, for this embodiment.

Q. Okay. So if the individual had two or more records with the same encrypted identifier, the data aggregator would be able to correlate them and determine that they pertain to the same person, correct?

A. Well, the ID would match. So then the aggregator can do whatever it wants to do with that information, but it would know -- or reasonably know that that was the same individual.

Q. Then at line 16, again in Column 12, Evenhaim discloses that, "Special care must be taken that the entity performing the linkage is not capable of knowing the key and decryption function because knowing these facets would enable a breach of the individual's privacy," correct?

A. That's what it says for that embodiment, yes.
Q. How would knowing the key and decryption function allow the entity that performs the linkage to breach the individual's privacy?
A. It could decrypt the identifiers.
Q. And by decrypting the identifiers, how would that breach the individual's privacy?
A. If the identifier contains PII, then it would be covered by HIPAA.
Q. Further down in Column 12 at line 26, Evenhaim discloses that, "There are numerous locations where an encryption of individual identification and/or merger of data for individuals could be facilitated."
Do you see that?
A. Yes.
Q. Evenhaim notes that encryption or merger can occur on the aggregator processor side or the source-entity processor's side; is that correct?
A. Yeah. As we've been discussing, those functions can be formed -- or be performed any number of places on that side of the security boundary.
Q. When you say "on that side of the security boundary," what's encompassed on that side of the security boundary?
A. Access to PII, as we've been discussing, can

occur on the aggregator and on the data sources. So depending upon how the system is architected, it's necessary to protect that information to comply with the law.

Q. So what entities do you consider to be within the same security boundary?

A. Well, anybody who has access to the PII. That's what we're trying to secure here.

Q. So who would those entities be in Evenhaim?

A. You already asked me that, but it would typically be things like hospitals and doctors.

Q. Evenhaim discloses that the data source entities provide de-identified data to the data aggregator, correct?

A. That's one of the ways they could do it.

Q. And so in that case, the data source entities and the data aggregator would not be within the same security boundary; is that correct?

A. They would be at different levels of security, but they would still have security requirements. So, I mean, arguably, that would be different domains, but they would still have security requirements placed upon them.

Q. So is there a provision of HIPAA that you're aware of in which an entity that only receives

de-identified data would be subject to the HIPAA privacy rule?

A. If it only has access to de-identified data, it's not covered. As we discussed, it's possible for places like insurance companies to process both.

Q. One moment. I'm just gathering my notes here.

So am I correct in understanding from your declaration that, in your view, Evenhaim's disclosure of the data aggregator performing encryption supports an understanding that Evenhaim's data sources would perform what you call token matching to identify individual patient records?

A. That's one possible way it could do it for sure since it has an encryption capability. It could de-identify the information before querying it if it wanted to.

Q. I'm sorry, what would de-identify the data before querying?

A. The aggregator certainly has the capability to do so because it has encryption and decryption functions.

Q. But the aggregator would not need to do so, correct?

A. It depends on the design of the database.

Q. And the queries are --

I'm sorry, go ahead.

A. In order for the system to function, it's going to have to create meaningful queries on fields that can be matched. And those can be, as we've discussed, matched on the aggregator, or they could be matched at the data sources depending upon the fields and the protocol that's being used.

Q. The queries are sent to the data source entities, correct?

A. Yes.

Q. And the data source entities are covered entities under HIPAA, correct?

A. Generally speaking, yes.

Q. And so the data source entities would, themselves, maintain PII for patients, correct?

A. Well, that's sort of the point of the reference, right?

Q. And so a query that's sent from a data aggregator to a covered entity would not need to de-identify patient data, correct?

A. It depends. As I said, the disclosure in the embodiments in Evenhaim allow for both possibilities.

Q. So in the embodiments in which you say that token matching would occur at the data source entities, would the data sources encrypt PII using the same

encryption key as the data aggregator to produce matching tokens?

A. Well, they would need to generate similar IDs somehow. But certainly it's possible that the systems that they would make available to the aggregator had been de-identified from their internal sources. It's not ruled out by the reference by any means.

Q. And so in those embodiments, again, would the data sources be capable of determining the identities of the individuals from the tokens it receives from the data aggregator?

A. Again, it depends. The key management scheme and everything else would play a role in what anybody could access, but it's -- the reference allows for you to create those tokens wherever you wish.

Q. If the data source entity maintained a record that associated the patient's identity with a token and then it received a matching token from the data aggregator, would the data source entity be able to use the token from the data aggregator to identify the individual?

MR. OLIVER: Objection. Form.

THE WITNESS: I mean, anything is possible. It depends on how the system is set up. If I were their security consultant, I'd probably have some process

separation, but people do different things.
BY MR. STEPHENS:
Q. But there's no such process separation disclosed in Evenhaim, correct?
A. It merely focuses on securing the PII and various ways and places that you can do that.
Q. And, again, in these embodiments, would the data sources return tokens with the de-identified patient records to permit the aggregator to link records to the same individual?
A. That's one possible way to do it, yes.
Q. Are there any specific examples in Evenhaim that you can identify where the data sources match tokens received from the data aggregator to de-identified patient data?
A. I think we've already discussed some of those, right, that the de-identification and, as you call it, the crunching could occur on the source entity or at the aggregator.
So in the cases where that occurred at the source entity, then they would be sending back the tokens to be linked by the aggregator.
Q. And I guess I'm not asking about the identification.
I'm asking if there are any specific examples

that you can point to in Evenhaim where the data source entities match a token received from the data aggregator to a corresponding token maintained by the data source entity?

A. If the tokenization occurs at the data source entity, that's the way it would have to work for the system to function. You can't match otherwise.

Q. But that's not expressly disclosed in Evenhaim?

A. It is. That one of skill in the art would know that, if that's storing tokens in the database at the source entity, that that's the way it would have to function. Otherwise you couldn't match.

Q. I'm not asking about what a person of skill in the art would -- would or would not have known.

I'm asking if there's an express disclosure in Evenhaim of matching performed at the data source entities. Are you able to point to any?

A. Yes, they're storing the database, and in order to query the database, you have to match. That's the way the system has to function.

Q. So, again, you're saying what has to occur and what a POSITA would understand.

I'm asking for specific examples expressly disclosed in Evenhaim.

A. And I've answered that question about four or five times now. I'll do it one more time.

That there is express disclosure of the case where the tokens could be on the source entity side, in which case that matching the query of that data would have to occur there. Then that's an express disclosure.

Q. And can you point me to that express disclosure?

A. I've already done so.

Do you want me to search again?

Q. Yes, please.

A. So Column 7, starting at about 39, it describes how the source entities could protect the privacy of the PII fields, which they would do by creating a token.

So there's your explicit disclosure.

Q. There's no express disclosure of a token in this portion, correct?

A. It doesn't use the word "token." It talks about using privacy-identified fields and creating a single unit. I would understand that to be a token.

I mean, if you're looking for the word "token," it's not there, but we have an understanding of what a token is by the construction.

Q. And this discussion pertains to alleged prior

art that's distinct from Evenhaim's present invention, correct?

A. Not distinct necessarily. These are systems that may need to be, in fact, supported by Evenhaim. So it acknowledges that they exist.

Q. Were there any other portions of Evenhaim that disclosed matching at the source entities?

A. There may be. That's the one I found. I'm not really inclined to search the whole reference.

Q. Are you aware of any other citations in your declaration to portions of Evenhaim disclosing matching of the source entities?

A. Not from memory, no.

Q. All right. Let's turn to your declaration, please.

A. Okay.

Q. And paragraph 40.

Are you there?

A. I am.

Q. And towards the bottom of page 20, in paragraph 40, there's a sentence that says, "Aside from the guidance in Figure 4, a POSA would also understand that, in order to comply with HIPAA, the query sent from the aggregator to the data sources should not include personally identifying information."

Do you see that?

A. Yes. That's the case where the token is, in fact, on the source entity.

Q. Are you aware of any provisions of HIPAA that would be violated by a noncovered entity transmitting PII to a covered entity?

A. I don't think the noncovered entity is allowed to have the PII.

Q. And by "PII," I'm referring to patient names, for example, decoupled from medical data.

A. Well, that's not what HIPAA defines it as. It's personally identifiable information. So it's information that allows you to deduce the identity of the individual, and that's not just names. There are other ways to do that.

Q. Sure. So I'll rephrase my question.

Are you -- are you aware of any provisions of HIPAA that would be violated by a noncovered entity transmitting patient names to covered entities?

A. I mean, I'd have to look at the specific example. But if you just sent the name and didn't have the healthcare data with it in any way, then it wouldn't violate. But if you link that with any medical procedure or any healthcare information, then you would have a HIPAA violation.

Q. Would you agree that the data aggregator in Evenhaim can transmit a patient list to the data sources without any medical information for the patients?

A. I'm sure that's possible. I mean, there's -- again, there's multiple embodiments disclosed in Evenhaim.

Q. And there's no express disclosure in Evenhaim of the data aggregator transmitting medical data to the data sources, correct?

A. I don't know. I haven't searched for that. I mean, it's certainly possible that it could. It would depend upon the query that was generated. I mean, it might -- I could imagine a situation where the patient list in a particular medical procedure would be transmitted.

Q. But, again, no express disclosure in Evenhaim of that situation, correct?

A. I'm not sure that's true. I mean, we can sit around and go search it again, but it's certainly the possibility that's allowed for.

Q. Let's take a few minutes. If you could identify any examples for me, that would be helpful.

A. Well, Figure 4 is showing a pharmaceutical company that's looking for certain drugs associated with certain names. So in that case, that would be part of

1 the query coming across.
2 Q. Can you point to that -- I'm sorry, that
3 portion of Figure 4 that you were referring to again?
4 A. The pharmaceutical company is requesting
5 information on patients and medications. So that would
6 be medical information associated with an individual.
7 That would be part of the query.
8 Q. So the query would identify the medications
9 that are of interest, correct?
10 A. And the individual.
11 Q. Correct.
12 But it does not identify that those
13 individuals have taken that medication, correct?
14 A. No, that's the query. So the Crossix server
15 is going to have to send that information when it's
16 querying the covered entities.
17 Q. And so are you saying that a query that
18 includes information about what medical information is
19 sought would be covered by HIPAA?
20 A. That's not what I said.
21 I'm answering your question, and your question
22 was provide an explicit disclosure where the patient
23 list and medical information would be part of the query.
24 And that's what I just gave you.
25 Q. And, yeah, I'm trying to understand this

example.

So with the medical information that you've given in Figure 4, is that a type of information that would require protections under HIPAA?

A. Yeah. If a -- if a person is taking a certain medication, that's definitely protected by HIPAA.

Q. But the information about whether the patients are taking the medications, that's not contained in the query, correct?

A. It is going to be -- not whether they are. The answer to the query is stored in the data source.

Q. Right.

So the query itself doesn't contain the patient's medical data records, correct?

A. It's going to include medical data and then an answer. So asking the question would necessarily transmit the information about the medical data being sought.

Q. But the query itself does not contain records of the patient's medical history, correct?

A. No. The answer to the question does. And so you asked for when medical information would be included with the patient list. And that's the example.

Q. All right. I think I understand. Thank you.

Going back to your declaration, then, at

paragraph 42.

Let me know when you get there.

A. Okay.

I said okay.

Q. I'm sorry.

In this paragraph, you refer to an additional level of security that could be added to the '641 patent in Evenhaim; is that correct?

A. Sure.

Q. And can you describe this additional level of security?

A. Yeah. I mean, as we've discussed, you can do multiple levels of encryption if you wish, using different keys and different tokens. It depends upon the granularity of the system that you're trying to provide.

Q. This additional level of security that you've described in paragraph 42 is not described in Evenhaim itself, correct?

A. I don't have complete recollection. It certainly allows for it. I mean, as we've been discussing, you can do things like super encryption. It would depend upon the requirements of the system you had built.

Q. You have no citations to Evenhaim in

paragraph 42; is that correct?

A. I don't see any.

Q. Are you aware of any disclosure in Evenhaim that provides this additional level of security?

A. Well, it, as we've discussed, allows encryption to occur at the data source and also at the aggregator, so I would understand that to allow for multiple encryptions.

Q. All right. Let's go forward to paragraph 86, please.

Are you there?

A. Almost.

Okay. I'm there.

Q. So in this paragraph, you indicate that, in the absence of token matching, there would be a need for, quote, "repeated encrypting and decrypting of the patient names. To comply with HIPAA" --

Do you see that?

A. Yes.

Q. Can you explain the basis for your statement there?

A. I don't understand your question.

Q. Yeah. Why would there be a need for repeated encrypting and decrypting?

A. Well, if you're going to have to create the

token every time the name comes across, then you would repeatedly encrypt and decrypt in order to match.

Q. Could you avoid the repeated encryption and decryption simply by not encrypting the individual patient names and the request sent from the data aggregator, apart from encryption of the message for data transmission security?

MR. OLIVER: Objection. Form.

THE WITNESS: I mean, any -- anything is possible. But I don't -- I think, if you're going to match the tokens as we understand the term "token" to mean, you're going to have to encrypt the PII and decrypt.

BY MR. STEPHENS:

Q. Why would you have to decrypt? I'm sorry. Can you clarify?

A. In order to match?

Q. Yes.

A. Because it depends on what's on the other side of the database. If it is not storing tokens, then you're going to have to match by name. Right? Or some other PII.

Q. And is the problem of repeated encryption and decryption disclosed anywhere in Evenhaim?

A. I -- I don't think it is specifically

disclosed there. It is just what one who was implementing the system would understand.

MR. STEPHENS: All right. I am about ready to transition to another reference. Maybe this would be a good point for, say, a five-minute break.

THE WITNESS: If you wish. Yeah. I'd probably do more like ten again, but that's fine.

MR. STEPHENS: Yeah, how about we reconvene at noon Eastern.

THE WITNESS: Okay.

(Recess: 11:47 a.m. to 12:06 p.m.)

BY MR. STEPHENS:

Q. I'd like to turn to the Murphy reference, which is Exhibit 1009.

Let me know when you have that document available.

A. Just digging for it.

All right. Go ahead.

Q. You're familiar with Murphy, correct?

A. Yes.

Q. Did you review Murphy while preparing your declaration?

A. Yes.

Q. Have you read Murphy in its entirety?

A. I've certainly scanned it. I'm not -- it's a

pretty long document, but I'm pretty sure I looked through all of it, yeah.

Q. How did you first encounter the Murphy reference?

A. It was provided by the attorneys.

Q. To the best of your recollection, were you aware of Murphy before your involvement in the present proceeding?

A. I don't think so. I was looking at the conference to see if it was one that I attended, but I don't think it was.

Q. Do you believe you have a good understanding of the technology described in Murphy?

A. A reasonable understanding. I mean, it was used for one particular claim limitation, so -- but I'll be happy to answer whatever questions you have.

Q. All right. Yeah. Let's turn to page 555 of Murphy.

Are you there?

A. I am.

Q. All right. I'll have some questions about the discussion on page 555. If you'd like to take a moment to review, please feel free.

A. Okay.

Okay.

Q. And so Murphy describes a query tool, correct?
A. Yeah. A query tool for examining de-identified information.
Q. And in this section on page 555, Murphy describes a desire to obfuscate the results provided by the query tool, correct?
A. Right. It does -- it doesn't want you to be able to zero in on one particular individual.
Q. And so the result that Murphy's query tool provides is a number of patients that satisfy the parameters in a search request; is that correct?
MR. OLIVER: Objection. Form.
THE WITNESS: Well, in particular, it's not gonna return with less than three records is the limitation so that the repeated queries don't allow you to single out one individual or two individuals from which you could determine the PII they say.
BY MR. STEPHENS:
Q. In the last paragraph on the left-hand side --
Excuse me. I'm going to take a drink of water, if that's all right.
All right. I'll restart my question.
In the last paragraph on page 55 [sic] on the left-hand column, beginning "one [sic] final solution," Murphy explains that his final solution was randomizing

the output within a certain range using a Gaussian function, correct?

A. Yes.

Q. How does the -- can you explain how the Gaussian function is used to randomize and thereby obfuscate the results?

A. I cannot.

Q. Do you have an understanding of what Murphy is likely referring to here?

A. Yeah. I mean, they're attempting to randomize, and there are a number of ways -- evidently, using a Gaussian function is one -- to randomize the output so that you are forced towards a mean, according to them.

But this is one final solution. That's not necessarily required.

Q. And, again, why is Murphy trying to randomize the output?

A. It's seeking to prevent inference of the PII. So one of the solutions is to not return less than three results, and the other one that they offer up is to randomize the output.

Q. So the obfuscated result then obfuscates the true number of patients in the group that are identified in response to the query?

A. I mean, that's one possibility.

Q. Okay. Then the -- and the right-hand side of page 555, about a third of the way down, Murphy says, (as read) "We modify our range algorithm to have a wider obfuscation at values close to zero and indicate the greater range by returning '<3' when the obfuscated number is less than three."

Is that right?

A. That's what it says.

Q. So if Murphy -- is it your understanding that Murphy produces the obfuscated number when the obfuscated number is not less than three?

A. I think it allows for that possibility. But here specifically, it says, (as read) "When the obfuscated number is less than three," is what the sentence says.

Q. Right. So when the obfuscated number is less than three, then it returns an indication of the range as less than three, right?

A. That's what it says.

Q. But when the obfuscated number is not less than three, then it produces a result that it's just the obfuscated number itself; is that right?

A. That's one possibility. I mean, it can -- basically the limitation that we were seeking to find

was an explicit disclosure in the field of limiting the number of records returned, and this provides it.

Q. So Murphy -- but it returns a response to the query regardless of whether the obfuscated number is less than three, equal to, or greater than three; is that correct?

A. No. That's not the way I understand that.

I understand that, if it's less than three, it tells you it's less than three. So it's limiting the number.

Q. And when the number is greater than three, a possibility is for Murphy to provide the number, the obfuscated number, correct?

A. That's one of the possibilities that it discloses, yes.

Q. Okay. Let's turn to the Dick reference, Exhibit 1007.

A. All right.

Q. I'm going to ask the same questions I've asked with respect to Evenhaim and Murphy.

So did you review Dick while preparing your declaration in this proceeding?

A. Yes.

Q. Have you read Dick in its entirety?

A. Yes.

Q. How did you first encounter the Dick reference?
A. This one was provided by the attorneys as well.
Q. To your recollection, were you aware of Dick before your involvement in the present proceeding?
A. I don't think so.
Q. And do you believe that you have a good understanding of the technology described in Dick?
A. Yes.
Q. I'd like to turn to Figure 3, please, of Dick.
A. Okay.
Q. And Figure 3 generally describes the system for requesting and retrieving medical information, correct?
A. Yes.
Q. Dick's system can process requests for de-identified medical information and can return such information in response to requests, correct?
A. That's one of the things it describes, yes.
Q. And in Figure 3, there are multiple components to a system, correct?
A. Yes. Different -- it discloses sort of a high-level architecture and functions.
Q. One of those components is a requesting and

viewing client, correct?

A. Yes.

Q. There are three different options disclosed. A first option, client/server; a second option, intranet based; and a third option, internet based; is that correct?

A. Those are the ones that are shown. There could be others.

Q. What is the function of the requesting and viewing client in Dick?

A. It's submitting queries.

Q. So, for example, the requesting and viewing client, 215, would submit a request to the requester's server; is that correct?

A. It would be routed through the requester's server, but, yes.

Q. And the request would be routed through the requester's server to the Central Server?

A. That's correct.

Q. What is the function of the requester's server, 230, in Dick?

A. It routes the request to the Central Server.

Q. Are there any other functions disclosed for the requester's server in Dick?

A. I don't know. I don't have total

recollection. I can search it once again, if that's where you want to go.

Q. Sitting here right now, you don't recall any other functions?

A. No, I don't have total recall of the reference.

Q. And the system further includes a Central Server, 245, correct?

A. Yes, as we discussed.

Q. There are four dashed boxes showing the Central Server that describe different functions of the server.

Do you see that?

A. Yes.

Q. And so the Central Server is responsible for formatting a query based on requests received from the requesting and viewing client; is that correct?

A. That's one of the things it can do, yes.

Q. Is there a difference between a request and a query in Dick?

A. I think so. I think the query is formatted according to the protocol. The request is probably a higher-level request.

Q. And how would the query be formatted according to the protocol?

A. Well, it would depend upon the back-end databases. It would be similar to the aggregator that we discussed at some length in Evenhaim where you have the Central Server that has to create a meaningful query that the -- will produce results from the databases it's talking to.

Q. And so the Central Server would format a query based on a receipt for request and forward the query to the archived medical information system or the medical information repository; is that correct?

A. Yeah. Those are the back-end data sources.

Q. Do you understand that Dick uses the shorthand AMIS, or A-M-I-S, for archived medical information system?

A. I've seen that, yes.

Q. Okay. And then similarly, MIR for the medical information repository?

A. Yes, I've seen that too.

Q. Dick, at paragraph 28, gives some examples of the medical information repository.

Let me know when you see that.

A. I'll scroll.

Q. Sure.

A. All right. Give me a moment.

Okay.

Q. And so some of those examples include a pharmacy benefit manager, a pharmacy -- physician's office, or clinical laboratory that stores identified patient information; is that correct?

A. Yes. Physician's office is also listed.

Q. The medical information repository would then be a covered entity under HIPAA?

A. If it has PII, it is for sure.

Q. Same as the archived medical information system?

A. If it has PII in it, then it's covered.

Q. And what's the difference between the archived medical information system and the medical information repository intake?

A. The difference listed is that the AMIS server can archive for longer periods of time than the MIR, but there may be other differences.

Q. The query that's transmitted from the Central Server could be queried to either the archived medical information system or the medical information repository?

A. I mean, according to the diagram, it looks like it could be passed through, yeah.

Q. The Central Server, as we mentioned earlier, receives the request and then formats the request for

the query, right?

A. That's the way I would expect it to work, yes.

Q. Are there any other components of the system that format the request for the query?

A. I mean, it's certainly allowed by the reference.

Q. But it -- are you aware of any disclosure in Dick of anything except for the Central Server formatting a request for the query?

A. Well, the database is, again, on the back side for the AMIS and the MIR. They are going to do some sort of formatting depending upon what type of DBMS and searching that they are doing.

So, yeah, I would expect some processing to occur on those systems.

Q. Some processing to occur at which system?

A. AMIS and MIR, depending upon where the query goes.

Q. The requester's server is never disclosed in Dick as formatting a query for the AMIS or the MIR, correct?

A. I don't remember an explicit disclosure on that. It is certainly possible. I wouldn't expect it to work that way.

Q. So after the Central Server sends a query to

AMIS or MIR, AMIS or MIR will return a result to the Central Server; is that correct?

A. Well, that's where they have the data. So they are going to have to provide that data in response to the query.

Q. And they provide the data back to the Central Server?

A. Yes.

Q. And the response that AMIS or MIR provide to the Central Server, is the medical information de-identified?

A. That's certainly possible.

Q. And I'll -- I guess I'll clarify.

Would it be de-identified when the patient has not provided authorization for the release of PII?

A. That would be a reasonable way to do it, yes.

Q. And is that what Dick discloses happens?

A. That's one of the possibilities, yes.

Q. Is there a difference between a possibility and what Dick discloses?

A. Yeah. I mean, again, it's disclosing an architecture for a system. And as we've discussed a fair amount, I mean, it's possible to move functions across servers when you're -- when we actually go to implement one of these systems.

Q. As Dick describes the embodiment that's shown in Figure 3, do the AMIS and MIR --

(Court reporter requested clarification.)

BY MR. STEPHENS:

Q. Does Dick describe in the embodiment of Figure 3 that AMIS or MIR returns de-identified patient data to the Central Server?

A. I'm looking.

Well, the description in Figure 3 says it -- Figure 3 illustrates several preferred physical environments in which the method of the preferred embodiment may be carried out. So by definition, we know that we can move those functions around is what that disclosure is telling us.

Let me see if I can find something even more explicit for you.

Yeah, it says at 24 that the identification could be done by patient number, which would be de-identified. So it certainly allows for that possibility.

Q. Does paragraph 45 also support that the medical information repository would return de-identified data?

A. Let's see what 45 says.

Well, that -- 45 is referring before it can be

released back to the requesting client. So it looks to me like it could be either/or as far as the AMIS and MIR are concerned.

Q. And how is the response to the query routed back to the client in Figure 3?

A. I understand it to be going through the Central Server to the requester's server.

Q. And the requester's server then forwards it to the requesting client?

A. Yes, unless -- I mean, you can also look that the intranet and internet connections go through the firewall to that server. So, I mean, there's some ambiguity there. But if I were implementing the system, they would all work the same way.

Q. And then the patient data would be -- would be de-identified when it reaches the requester's server, correct?

A. Unless there's a signed authorization form with it.

Q. Right.

Would a POSITA understand the requesting and viewing client is a noncovered entity?

A. I mean, that's one possibility. I wouldn't say it has to be that way.

But, I mean, it -- it would be possible to

implement this system in such a way that the requesting client wasn't covered.

Q. And similarly, it would be -- would it be possible to implement the system in a way that the requester's server is not a covered entity?

A. Yes. For the same reasons.

Q. And likewise, would it be possible to implement the system where the Central Server, 245, is not a covered entity?

A. I mean, anything is possible. That's going to be harder. Like I said, this -- the Central Server is like the aggregator of Evenhaim.

So, in general, it has to be trusted, but it would be possible -- I mean, you could implement and architect the system in such a way that it never processed PII.

Q. Does Dick disclose any methods for de-identifying patient data?

A. I'm going to have to search the whole document. I don't have recollection of specific methods.

I mean, a person of skill certainly would know what cryptographic methods were available. But let me search.

Q. Yeah. I think I'll -- I'm thinking of

paragraph 45 as one example.

A. All right. Let's have a little reading.

Well, 45 says "de-identifying methodology," which is what I said. I mean, any number of way cryptographic mechanisms are known to do that.

46 says --

Well, I'm not finding a reference to hash or encryption. So it -- it may be that it assumes the knowledge of the reader as to what -- to know what de-identifying methodologies are.

Q. Would a person of skill know how to implement the de-identifying methodologies?

A. Should.

Q. And could those methodologies include things other than encryption and crypto -- I'm sorry, cryptographic techniques?

A. I mean, it's certainly possible that you could use other types of IDs or pseudonyms for PII, but generally speaking, I think they would use cryptographic mechanisms.

Q. Would a person of skill see a need to look beyond the Dick reference itself to implement de-identifying methodologies?

A. No. I think a person of skill would have knowledge of HIPAA and the need to de-identify data.

And, I mean, any number of libraries that are out on the Internet to do that.

Q. All right. Could we turn to the Landi reference, Exhibit 1008.

A. All right. Got it.

Q. You're familiar with the Landi reference, correct?

A. Yes.

Q. Did you review Landi in the course of preparing your declaration?

A. Yes.

Q. And have you read Landi in its entirety?

A. Yes.

Q. How did you first encounter the Landi reference?

A. This is another one provided by the attorneys.

Q. To your recollection, were you familiar with Landi before your involvement with this IPR?

A. I don't think so.

Q. And do you believe you have a good understanding of the technology described in Landi?

A. Yes.

Q. At Column 1 of Landi, around line 12, there's a section that's titled "Technical Field of the Invention."

Do you see that?

A. Yep.

Q. And this section describes what the present invention relates to, correct?

A. I mean, it's -- the field of the invention is the protection of privacy of healthcare data is what it says.

Q. Starting at line 16, it says, "In particular" -- it's carrying over from the present invention -- "in particular, to systems and methods that implement secured key encryption for de-identifying patient data to ensure patient privacy while allowing only the owners of the patient data records and/or other legally empowered entities to reidentify subject patients of de-identified data records when needed."

Do you see that?

A. That's what it says.

Q. Why would the owners of the patient data records or other legally empowered entities need to reidentify the patients?

A. Any number of reasons. I mean, if you had a data coherency problem, you might want to undo the de-identification so that you could fix the coherency of the database, for instance. It also --

Q. All right.

Oh, go ahead.

A. -- looks like there's -- looks like there's law, legally empowered entities, I would assume maybe to be law enforcement or something like that or Court order.

So those -- those would be entities that might have a need to reidentify the data.

Q. Would you agree that a central focus of Landi was allowing for reidentification of patients?

A. No. I think that that's a feature of using reversible encryption, but I don't think that was the focus. The focus is protecting patient privacy.

Q. And Landi identified reidentification as an aspect of his invention, correct?

A. Right. If you use reversible encryption, then reidentification is possible if you get access to the keys.

Q. So reidentification would be possible if you had the patient's de-identified data record, the encrypted ID, and a decryption key?

A. And the algorithm for the --

(Court reporter requested clarification.)

THE WITNESS: The algorithm for the encrypted data.

BY MR. STEPHENS:

Q. All right. Let's turn to Figure 1, please. Are you there?
A. Almost.
Q. Sure.
A. Okay.
Q. And so Figure 1 provides an overview of the system disclosed in Landi, correct?
A. Yeah. It's a high-level architecture diagram, if you will.
Q. And that diagram shows a set of patient data processing systems, 20-1 through 20-n, correct?
A. Yes.
Q. The system further includes a central patient data processing system, 30; is that correct?
A. Yes.
Q. And then a central surveillance system, 50, correct?
A. Yes.
Q. And the patient data processing systems, 20, are operated at different clinical sites by different healthcare organizations, correct?
A. For this embodiment, yes.
Q. The patient data processing systems maintain identified patient data, correct?
A. That's what's shown in this particular figure,

yes.

Q. And the identified patient data is indicated by 21; is that correct?

A. I don't understand your question.

Q. Yeah. I'm sorry.

Within patient data processing systems, 20, there's a cylinder labeled "21" that's -- or numbered 21 that's labeled "Identified Patient Data."

Do you see that?

A. I do.

Q. And so what would be contained in the identified patient data repository?

A. I understand that to be data that needs to be protected. So it would have PII in it.

Q. So the patient data processing systems are analogous to the medical information repository in Dick, in that they both maintain identified patient data?

A. Yeah. They could actually be both -- since the MIR and the AMIS are passing information back and forth, this could fulfill actually both functions.

Q. I'm sorry. What do you mean by "both functions"?

A. You were asking me how this maps to Dick, and I'm saying this is -- the servers that contain the PII in Dick would be represented here.

Q. Right. Like the medical information repository in Dick?

A. Or like the AMIS in Dick, yes.

Q. Yes.

And Landi discloses that the patient data processing systems can produce de-identified patient data using an encryption system; is that correct?

A. That's the intent of this embodiment, yes.

Q. How does the encryption system work in Landi?

A. It has -- it's a public key-based, key-management system.

Q. And so how does the encryption system generate an encrypted ID for the patient data processing systems?

A. It would encrypt with a public key at some level.

Q. That encrypts PII with the public key?

A. That's one way to do it. It can also encrypt -- you've also got a key generation engine down there, so it could be that you were generating symmetric keys that were used to encrypt the data that were then encrypted with the public key.

But essentially the public key -- or the private key would control access to that data after it's encrypted.

Q. And the encryption systems are located in the

patient data processing systems in Landi; is that correct?

A. That's where the actual encryption occurs, yes.

Q. There's no other use of the encryption systems outside of the patient data processing systems, correct?

A. For this embodiment, the encryption is controlled within those systems so that the -- what is released is de-identified patient data.

Q. And the de-identified patient data is then released to the central patient data processing system?

A. Right. That's the -- that's where the queries would be matched.

Q. And the central surveillance system, 50, includes a master private key.

Do you see that?

A. I do.

Q. What would the master private key be used for?

A. As I said, depending on how it's implemented, it would probably be used to access individual symmetric keys that were used to do the encryption, but it could also be used to access and reidentify patient data is essentially what its use is.

Q. The patient data processing systems -- going back to the top of the figure -- those would be covered

entities under HIPAA, correct?

A. If they have PII, they are covered.

Q. And then the central patient data processing system, 30, would not be a covered entity under HIPAA; is that correct?

A. It may, or it may not be. Again, to the extent it has access to PII because it's talking with the server that has the master private key, then it would be covered. But, I mean, there are a variety of ways to implement this architecture.

Q. As shown in Figure 1, there is no identified patient data repository within the central patient data processing system, correct?

A. That doesn't mean that it doesn't have access to the PII.

Q. But it's not shown in Figure 1?

A. It is shown, to somebody who understands the key management and cryptography, that it's possible for 30 to have access to PII by virtue of the data flows that exist.

Q. Again, is there any disclosure in -- in Landi that -- in which the central patient data processing system has identified patient data?

A. Yes, as I've just described to you.

Q. So you are inferring that from the

communications?

A. I'm not inferring anything. As a person well versed in cryptography, I'm telling you that it's possible, depending upon those data flows, for the server, 30, to have access to PII, which would make it covered.

Q. Would you agree that just because something is possible does not mean that it is disclosed in the reference?

A. No. I mean, if one of skill in the art would understand that disclosure, then it's disclosed.

Q. You're unable to point to any text in Landi in which the central patient data processing system includes identified patient data?

A. False. I just explained how it could have access to the PII.

Q. But you're not aware of any text that discloses identified patient data within the central patient data processing system?

A. I don't know if it goes through and explains it. I'm telling you what I'm looking at and what a person of skill would understand or a person who at least understands cryptography would understand this to disclose.

MR. STEPHENS: All right. It's 1:00 p.m.

Eastern right now.

Should we take a -- I think this would be a good time for a lunch break, if that's okay with you, Dr. Clark.

THE WITNESS: Depends on how much longer you want to go with this. If you think we're going to go a few more hours, then probably. If you're going to try and wrap up in another hour or so, then I'm happy to work with you and power through. It's up to you.

MR. STEPHENS: Why don't we take 30 minutes and reconvene at 1:30.

THE WITNESS: Okay.

MR. STEPHENS: Okay.

(Recess: 1:01 p.m. to 1:38 p.m. EST.)

BY MR. STEPHENS:

Q. All right. Welcome come back from lunch, Dr. Clark.

During the break, did you have any discussions about the substance of your testimony with anyone?

A. Nope.

Q. Let's turn to paragraph 214 of your declaration.

A. Okay.

Q. Okay. And this paragraph is in the context of your analysis of the Dick and Landi combination,

correct?

A. Yes.

Q. I have a few questions for you just to help clarify your understanding of what this combination is.

So as described at paragraph 214, we understand that, in this combination, you're proposing to implement Landi's encryption server and Dick's requester's server; is that correct?

MR. OLIVER: Objection. Foundation.

THE WITNESS: So can you re-ask your question? It was a little unclear to me.

BY MR. STEPHENS:

Q. What are you proposing to modify in Dick to integrate a requester's server -- I'm sorry, integrate an encryption server?

A. If we look at Figure 3, I mean, it's basically what you need is the token or de-identified database that Landi discloses and plug it into Dick, so there's multiple ways one might do that.

One is at the Central Server. You could also replace the requester's server, insofar as it's only routing information to. So the main idea is that you're replacing the PII-containing databases with those of Landi and then the token -- also the token system of Landi and plugging it into Dick.

And there's more than one way to do that, obviously.

Q. But as described at paragraph 214, you've proposed to place Landi's encryption system in Dick's requester's server; is that correct?

A. That's one way to do it. As I'm looking at it now, it's probably -- be even easier to just plug it at the Central Server. But either way would work.

Q. You did not describe the option of modifying the Central Server to include encryption server in your declaration?

A. Either one works. As we discussed, the requester's server is just routing the request. So you could -- you could plug in the system of Landi at either place, and it would function the same.

Q. And the system would still be HIPAA compliant even if encryption were performed at the Central Server rather than the requester's server?

A. As long as there -- the PII was protected and it was designed to only return de-identified information, yes, it would be compliant.

Q. And as a further modification of Dick's system, are you proposing that Landi's central patient data processing system could be queried in lieu of the AMIS or MIR?

A. Yes, absolutely, because the PII of Landi -- of Landi comes from those data sources, so the query would be routed to them. As I said, much the same as what we described in Evenhaim.

Q. And so the query -- would the query and the response follow a similar path as Dick describes through the requester's server -- Central Server and then to the central patient data processing system in your combination?

MR. OLIVER: Objection. Form.

THE WITNESS: Yeah. What -- the requesting client -- and you have three types -- would make a request through that would be routed to the system of Landi to satisfy it with de-identified information.

BY MR. STEPHENS:

Q. In the proposed combination, the response would be routed back to the requesting client through the requester's server; is that right?

A. Yes. So basically the data flows would be the same. It's just that you would have to have the de-identified information produced and then delivered to the client.

Q. And so that de-identified information in Landi is -- includes the encrypted ID, correct?

A. It could.

Q. In the combination, the encrypted ID would be routed to the requesting client through the requester's server?

A. That's possible, sure.

Q. That's consistent with your description of the combination?

A. I think so.

Q. Okay. Let's turn to the Settimi reference, Exhibit 1006.

A. Okay.

Q. And you're familiar with Settimi, correct?

A. Yes.

Q. Have you reviewed it in its entirety?

A. Yes.

Q. Were you aware, to your knowledge, of the Settimi reference before your work on this IPR?

A. I may have been, but it -- it was provided by the attorneys, in answer to your next question.

Q. All right. Let's take a look at Figure 2 of Settimi, please.

A. Okay.

Q. Can you describe what's shown in Figure 2?

A. It's the data architecture for that embodiment.

Q. There's a collection of PCPs shown in

Figure 2, correct?
A. PCPs, you mean?
Q. Yes.
A. Yes.
Q. The PCPs are patient care providers, correct?
A. Yes.
Q. And the PCPs communicate with the data warehouse system?
A. Yes.
Q. Which produces a patient cohort report, 212?
A. Yes.
Q. And then each of the PCP maintains an electronic medical records database, correct?
A. Yes.
Q. The PCPs release de-identified patient data to the data warehouse; is that correct?
A. In this embodiment, yes.
Q. Are there other embodiments of which you're aware in which the patient data is not de-identified before release to the data warehouse system?
A. I'd have to review the entire reference. I mean, that's the interesting one.
Q. But sitting here now, you don't recall such embodiments?
A. I don't have total recall of the reference,

no.

Q. The data warehouse system includes a data import function, 206.

Do you see that?

A. I do.

Q. And what does the data import function do?

A. It does the aggregation and deidentification of the patient data from the sites.

Q. Is that from paragraph 35?

A. That's from paragraph 35.

Q. Would aggregating patient data include merging patient data records?

A. It could include lots of things. I mean, data aggregation. I mean, they might change the structure. They do all sorts of processing on the data.

Q. Could you elaborate? What would aggregating data in this context mean to you?

A. I would think it would include linking things like canonicalization, other things that would make the system function better.

(Court reporter requested clarification.)

BY MR. STEPHENS:

Q. And in your declaration, you analyzed Settimi in the context of a combination with Evenhaim, correct?

A. Yes.

Q. Your declaration did not rely on Settimi as disclosing the encryption server; is that correct?

A. No. It was a combination to allow Evenhaim to query de-identified information.

Q. So the mapping through the encryption server in the Evenhaim/Settimi combination would be the same as your mapping in the Evenhaim first draft one.

A. Yes.

MR. STEPHENS: All right. I think we're near the end here.

Could we take ten minutes? I'll confer with our team and see if we have further questions.

THE WITNESS: Absolutely.

MR. STEPHENS: All right. Why don't we return at 2:05.

(Recess: 1:55 p.m. to 2:06 p.m. EST).

BY MR. STEPHENS:

Q. All right. Welcome back, Dr. Clark.

During the break, did you discuss the substance of your testimony with anyone?

A. Didn't discuss anything with anybody.

MR. STEPHENS: We have no further questions. We pass the witness.

MR. OLIVER: Thank you.

I have no questions for the witness.

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

MR. STEPHENS: Yeah. I think that, our order, we had asked for a rough in 48 hours and then final by October 3rd. Could we get the rough within 24.

COURT REPORTER: Yes.

MR. STEPHENS: And then final is still okay for October 3rd.

COURT REPORTER: Perfect.

MR. OLIVER: And I don't need a copy. There will be a copy made public in the file, so I'm good for right now. But thank you.

(Whereupon the proceedings concluded at 2:08 p.m. EST)

ERRATA SHEET

NAME OF CASE: DATAVANT, INC. V. VIGILYTICS LLC
DATE OF DEPOSITION: September 26, 2024
NAME OF WITNESS: DR. PAUL CLARK

Reason Codes:

1: To clarify the record.
2: To conform to the facts.
3: To correct transcription error.

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

Page _____ Line _____ Reason _____

From _____ to _____

_____ _____

DR. PAUL CLARK **DATED**

DECLARATION UNDER PENALTY OF PERJURY

I, DR. PAUL CLARK, do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on September 26, 2024; that I have made such corrections as appear noted on the Deposition Errata Page(s), attached hereto, signed by me; that my testimony as contained herein, as corrected, is true and correct.

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

_____

DR. PAUL CLARK

STATE OF CALIFORNIA))) ss.

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

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

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

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

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

In witness whereof, I have hereunto subscribed my name.

Dated: 3rd of October, 2024.

Tamara L. Houston

TAMARA L. HOUSTON
CSR 7244, RPR, CCRR 140

-

--o0o--
6:2

1

1
25:7 35:24 81:23 84:1,6 88:11,16

1001
9:2 25:8

1003
9:21 13:18

1004
16:13

1005
10:2 26:23

1006
10:6 94:9

1007
10:10 69:17

1008
81:4

1009
10:16 64:14

10:50
45:20

11:04
45:20

11:47
64:11

12
45:25 46:7 47:20 48:10 81:23

12:06
64:11

13
37:8 40:13 42:24 46:16

14
40:7 41:22

16
47:20 82:8

1995
15:1 17:25

1999
16:22 17:25

1:00
89:25

1:01
90:14

1:30
90:11

1:38
90:14

1:55
97:16

2

2
15:15 94:19,22 95:1

20
11:3 56:20 84:19 85:6

20-1
84:11

20-n
84:11

2000s
38:17

2009
21:25

2024
6:1

2024-00226
6:24 9:8

206
96:3

21
85:3,7

212
95:10

214
90:21 91:5 92:3

215
71:13

230
71:21

24
77:17 98:5

245
72:8 79:8

25
15:1,5,6

26
6:1 21:14,17 48:10

28
22:2 24:22 73:19

2:05
97:15

2:06
97:16

2:08
98:14

3

3
31:9 40:7 42:12,16 43:24 68:6 70:11,13,21 77:2,6,9,10 78:5 91:16

30
25:11 84:14 88:4,19 89:5 90:10

33
37:8

35
96:9,10

36
37:8

39
55:12

3rd
98:5,8

4

4
27:23,24 28:3,16 29:15 30:7 35:22 36:6,16 37:6 40:7 41:22 42:9,12 43:1,24 56:22 58:23 59:3 60:3

40
56:17,21

42
61:1,18 62:1

45
77:21,24,25 80:1,3

46
80:6

48
98:4

4A
27:24 28:8,13

4B
28:13

5

5
32:2,5 44:11,18 45:3

50
84:16 87:14

55
66:23

555
65:17,22 66:4 68:3

590
15:17

6

641
8:25 14:8 22:5 23:10, 14,24 24:8,17,25 25:7 61:7

7

7
13:17 35:24 41:23 55:12

8

86
62:9

9

9118641
6:24 9:3

9:38
6:1

A

A-M-I-S
73:13

a.m.
6:1 45:20 64:11

abovementioned
40:8

absence
62:15

absolutely
93:1 97:13

abstract
34:19

access
18:21 20:16 30:6,19,21, 24 31:2,3,5,12 34:22 35:21 36:8 48:25 49:7 50:3 52:14 83:16 86:23 87:20,22 88:7,14,19 89:5,16

accessing
31:22

accordance
21:23

accurate
8:13

acknowledges
56:5

acronym
9:11

ACSAC
20:9

actual
87:3

add
25:3

added
61:7

addition
40:4

additional
26:13 61:6,10,17 62:4

address
17:15

adopted
22:3,24 23:18 24:4,15

advised
41:23

aggregates
36:12

aggregating
96:11,16

aggregation
96:7,14

aggregator
28:10 30:8,11,15,24 31:5,25 32:9,17,20,22, 24 33:5,9,11,18,21 34:6,8,12,16,17,20,24 35:1,10 36:17 46:25 47:8,14,17 48:17 49:1, 14,17 50:9,19,22 51:5, 19 52:1,5,11,19,20 53:9,14,19,22 54:2 56:24 58:1,8 62:7 63:6 73:2 79:12

agree
22:12,18 29:14 42:15 44:18 58:1 83:8 89:7

agreement
22:16

ahead
51:1 64:18 83:1

AI
17:18

AI-GUIDED
17:14

aim
7:5,11

algorithm
39:12,16 68:4 83:21,23

algorithms
38:24

alleged
9:13 55:25

allowed
57:7 58:20 75:5

allowing
82:12 83:9

ambiguity
78:13

AMIS
73:13 74:15 75:11,17, 20 76:1,9 77:2,6 78:2 85:19 86:3 92:25

amount
76:23

analogous
85:16

analyses
22:15

analysis
23:16 36:14 90:25

Analyze
32:3

analyzed
96:23

and/or
48:12 82:13

answering
7:6 59:21

appearance
6:18

applied
21:22 38:21

apply
22:14,19,21 23:8 40:1 41:3 42:3

approximately
11:1 12:24 13:8 14:23 15:7,12

architect
79:15

architected
30:20 32:12 49:2

architecture
32:25 70:24 76:22 84:8 88:10 94:23

archive
74:16

archived
73:9,13 74:9,12,19

arguably
49:21

art
9:12 31:20 38:3 40:25 43:1,16 54:10,15 56:1 89:10

aspect
83:14

aspects
19:16 40:8

assistant
13:15

assume
24:20 83:3

assumes
40:16 80:8

attain
25:21

attempting
30:1 36:8 67:10

attended
65:10

attorney
6:11 11:25

attorneys
22:15 25:6 65:5 70:3 81:16 94:18

authentication
38:13

author
20:3

authorization
20:17 29:12 76:15 78:18

avoid
63:3

aware
14:10,15,16,18,19 27:11 30:23 31:4 49:25 56:10 57:4,17 62:3 65:7 70:5 75:7 89:17 94:15 95:19

B

back
15:1 34:18 35:22 36:14 37:4 42:9 53:21 60:25 75:10 76:6 78:1,5 85:19

87:25 90:16 93:17 97:18

back-end
73:1,11

background
14:1

Barclay
6:15

based
22:11 24:8 71:5 72:16 73:8

basically
17:1 68:25 91:16 93:19

basis
33:3 62:20

begin
13:8

beginning
66:24

begins
46:3

behalf
6:13,20

benefit
28:5 74:2

Bethesda
8:9

big
21:8

biggest
21:7

binder
7:19

bit
17:17 45:12,16

bits
39:15

books
38:14

bottom
56:20

boundary
36:25 37:1,3 47:6 48:21,23,24 49:6,18

box
32:5 44:14

boxes
72:10

breach
47:24 48:4,7

break
7:10,11,12 45:14,22 64:5 90:3,18 97:19

breaks
7:14

briefly
39:13

broad
26:18 44:25

broader
24:1

brought
16:16

brute
26:22

built
61:24

bullet
24:21

bunch
14:2

C

call
50:11 53:17

called
6:4 43:18

canonicalization
96:19

capabilities
30:14

capability
50:14,19

capable
47:22 52:9

capacity
11:13 12:1

care
47:21 95:5

career
14:23 19:3

careful
46:8

carried
77:12

carry
42:1

carrying
82:9

case
15:2,19,23,24 33:11 34:24 49:16 55:3,5 57:2 58:25

cases
53:20

caught
14:22

center
30:8

central
71:18,22 72:7,11,15 73:4,7 74:18,24 75:8,25 76:2,6,10 77:7 78:7 79:8,11 83:8 84:13,16 87:11,14 88:3,12,22 89:13,18 91:20 92:8,10, 17,23 93:7,8

CEO
17:8,14

change
96:14

changed
14:13

channel
40:22 41:16

characterizes
22:9 24:15

chief
18:1,5

choose
41:6

Christopher
8:7

cipher
39:16

circuit
46:11 47:2

citations
56:10 61:25

city
8:8

claim
21:20 22:4 25:7,13 65:15

clarification
16:1 25:4 40:17 77:3 83:22 96:21

clarify
63:16 76:13 91:4

clarity
8:15

Clark
6:3,9,25 8:7 16:18 34:10 45:22 90:4,17 97:18

class
46:4

clean
7:5

Clear
17:8,12,22

client
18:20 19:4,10,13 71:1, 10,13 72:17 78:1,5,9,22 79:2 93:12,17,22 94:2

client/server
71:4

clinical
74:3 84:20

clinician
17:20

close
68:5

co-authors
20:6

codes
38:13

coherency

82:22,23

cohort
95:10

collaborated
11:19

collaborative
12:12,15,21

colleagues
6:14

collection
94:25

column
37:8 40:7,13 41:22 42:24 45:25 47:20 48:10 55:12 66:24 81:23

combination
90:25 91:4,6 93:9,16 94:1,6 96:24 97:3,6

commercial
18:10

common
46:10,12,21 47:9

communicate
95:7

communication
8:2 36:22 40:14

communications
89:1

companies
17:5,6,23 21:7 50:5

company
17:1 19:8 28:4 29:15,20 36:8 37:6 58:24 59:4

compared
24:5

compensated
15:16,20

compensation
15:22

complete
28:22 30:25 61:20

compliance
19:14,22

compliant
19:18 92:16,21

comply
21:2 49:3 56:23 62:17

complying
29:6

components
70:21,25 75:3

compromising
46:12

computationally
25:21,22 26:9,11,22

computer
17:20 23:19,21 25:24

computing
28:4,9

concerned
19:5,11 78:3

concluded
98:13

conditions
43:19

confer
97:11

conference
20:2 65:10

conjunction
39:1

conjunctive
34:21

connections
78:11

considered
13:19,23

consistent
23:13,23 24:9,16,20 94:5

constructing
31:1

construction
21:20 22:24 23:5,12,19, 23 24:4,9,16,23 55:24

constructions
22:4,12,14,18,21

consultant
52:25

consulting
11:16 15:17

consumer
28:9 29:16,24 30:3

consumers
28:19,21 29:23

contained
14:8 60:8 85:11

contents
12:22 41:18

context
90:24 96:17,24

contingent
15:23

contradict
24:1

contradicts
23:17 24:12 44:7

control
20:15 86:23

controlled
87:8

controlling
18:21

copies
7:19,23

copy
16:13 98:10,11

correct
7:3,20 13:20 15:10,18 16:19,20 17:10 18:2,3 21:3,20,25 22:5,9,12 23:2,7,10,11,21 24:6,25 25:16 27:1 28:6,10 29:6 30:4,9,16 31:11 32:6, 10,22 33:5,6 34:17 35:15,24 36:18,22 37:18 40:15 41:4 42:1, 13 43:11 45:3 46:5,17 47:2,9,15,25 48:18 49:14,18 50:7,23 51:9, 12,15,20 53:4 55:18 56:2 58:9,17 59:9,11,13 60:9,14,20 61:8,19 62:1 64:19 66:1,6,11 67:2 69:6,13 70:15,19,22 71:1,6,14,19 72:8,17 73:10 74:4 75:21 76:2 78:17 81:7 82:4 83:14 84:7,11,14,17,21,24 85:3 86:7 87:2,6 88:1,5, 13 91:1,8 92:5 93:24 94:11 95:1,5,13,16 96:24 97:2

correctly
37:14 46:14

correlate
47:14

correlated
31:5

counsel
6:17 10:21 11:23 12:20, 25 13:5,14 22:20 45:23 98:1

countermeasures
39:1

couple
15:14 27:14

court
16:1,3,6,9 22:14 40:17 77:3 83:4,22 96:21 98:1,6,9

covered
20:19,22,24 21:4,10 29:8 30:4,16,21 36:8 48:9 50:4 51:11,19 57:6,19 59:16,19 74:7, 11 79:2,5,9 87:25 88:2, 4,9 89:6

create
25:1 31:3 35:19 51:3 52:15 62:25 73:4

creating
55:15,20

criticized
16:6

Crossix
28:5 30:7 31:21 36:9, 10,11 37:2 42:12 59:14

cruncher
32:6,8,16,21 33:4,8,12, 20 34:7 44:13

crunching

53:18

crypto
80:15

cryptographic
79:23 80:5,16,19

cryptographically
26:21

cryptography
88:18 89:3,23

CTO
16:18

curriculum
16:14

customary
21:23

customers
18:10

CV
17:10 19:24 20:9

cylinder
85:7

D

dashed
72:10

data
18:16,17 19:18 21:9 28:9,10,16,24 29:2,5, 10,15,24 30:2,3,8,11, 15,24 31:5,6,11,12,16, 24 32:1,4,6,8,9,16,17, 21,22 33:4,5,8,12,18, 20,21 34:12,13 35:1,6, 10,13,14 36:17,18,21 37:4,10,12,18,20,23 38:4,5,7,10,11,16,22 39:4,16 40:4,14,20,23 41:4,5,14,16 42:16,24 43:2 44:3,13 46:5,8,10, 16,17,19,25 47:1,8,13 48:13 49:1,12,13,16,17 50:1,3,9,10,17 51:6,8, 11,14,18,20,24,25 52:1, 9,11,16,18,19,20 53:8, 13,14,15 54:1,2,3,5,17 55:5 56:24 57:10,22 58:1,2,8,9 60:11,14,15, 17 62:6 63:5,7 73:11 76:3,4,6 77:7,23 78:15 79:18 80:25 82:6,12,13, 15,18,22 83:7,19,24 84:10,14,19,23,24 85:2, 6,8,12,13,15,17 86:5,7, 13,20,23 87:1,6,9,10, 11,22,24 88:3,12,19,22, 23 89:4,13,14,18,19 92:24 93:2,8,19 94:23 95:7,15,16,19,20 96:2, 6,8,11,12,13,15,17

database
30:12 32:12,25 35:20 43:5,11,17 50:24 54:11, 19,20 63:20 75:10 82:24 91:17 95:13

databases
18:16 30:20 36:12 73:2, 5 91:23

Datavant
6:20 8:17,18 11:13,16, 20

Datavant's
11:22

day
7:13

day-to-day
17:2

days
10:22

DBMS
75:12

DDMS
30:12

de-identification
18:17 19:17 27:14 41:15 53:17 82:23

de-identified
20:18 49:13 50:1,3 52:6 53:8,15 66:3 70:18 76:11,14 77:6,19,23 78:16 82:15 83:19 86:6 87:9,10 91:17 92:20 93:14,21,23 95:15,19 97:4

de-identify
50:15,17 51:20 80:25

de-identifying
79:18 80:3,10,12,23 82:11

dealing
19:22

declaration
9:19,20 10:23 11:6,9 12:8,12,15,18,23,25 13:9,15,17,20 14:4,9, 13,14,17,20 15:15 21:15,19 23:13 27:4 50:8 56:11,14 60:25 64:22 69:22 81:10 90:22 92:11 96:23 97:1

declarations
12:19

decoupled
57:10

decrypt
44:15,24 48:5 63:2,13, 15

decrypted
44:19

decrypting
48:6 62:16,24

decryption
37:13 47:23 48:2 50:20 63:4,24 83:20

dedicated
7:21,25 8:3

deduce
57:13

deemed
21:4

define
8:15

defines
57:11

definition
20:21 77:12

degree
37:18 40:14

deidentification
96:7

delivered
93:21

dep
7:22

depend
58:12 61:23 73:1

depending
32:24 42:6 49:2 51:6 75:12,17 87:19 89:4

depends
26:3 30:19 32:12 35:11 36:23 39:6,21,24 42:19 43:5 50:24 51:21 52:12, 24 61:14 63:19 90:5

depicted
29:15

deposed
15:10,13

deposition
6:12 7:2 9:17 10:20 11:2,5,10

derive
26:10

describe
10:19 12:7,14 18:7 20:13 36:1 39:13 61:10 72:11 77:5 92:9 94:22

describes
28:23 55:13 66:1,5 70:13,20 77:1 82:3 93:6

description
40:12 77:9 94:5

design
18:12,25 50:24

designed
43:6 92:20

desire
66:5

detect
24:6

determine
47:14 66:17

determining
52:9

developed
18:15

diagram
74:22 84:8,10

Dick
10:9 69:16,21,24 70:1,

5,9,11 71:10,21,24 72:20 73:12,19 75:8,20 76:17,20 77:1,5 79:17 80:22 85:16,23,25 86:2, 3 90:25 91:13,18,25 93:6

Dick's
70:17 91:7 92:4,22

dictated
40:24

difference
72:19 74:12,15 76:19

differences
74:17

digging
64:17

directly
23:16

disagree
22:18

disagreement
22:16

disclose
79:17 89:24

disclosed
33:4 53:4 54:8,25 56:7 58:5 63:24 64:1 71:3,23 75:19 84:7 89:8,11

discloses
37:9,17 46:8 47:21 48:11 49:12 69:15 70:23 76:17,20 86:5 89:18 91:18

disclosing
56:11 76:21 97:2

disclosure
30:23 31:4,15 32:15,21 33:7,10,24 34:5,9 37:25 38:1,9 42:23 44:6 50:8 51:21 54:16 55:3,6,8, 16,17 58:7,16 59:22 62:3 69:1 75:7,22 77:14 88:21 89:11

discuss
45:22,24 97:19,21

discussed
50:4 51:5 53:16 61:12 62:5 72:9 73:3 76:22 92:12

discussing
48:19,25 61:22

discussion
55:25 65:22

discussions
90:18

disseminated
20:18

distinct
56:1,3

division
18:6

doctor's
29:1

doctors
49:11

document
64:15 65:1 79:20

documents
7:20,23 11:4 12:10 13:18,22,25 14:3

DOD
18:10

domains
49:21

dozen
15:4,14

draft
97:7

drafted
12:25 13:5

drink
66:20

drugs
58:24

duly
6:4

duration
7:22

Dyncorp
18:1,6,8,11,23

E

earlier
74:24

early
38:17

easier
92:7

Eastern
64:9 90:1

effort
12:12,15,21

either/or
78:2

elaborate
17:17 25:22 41:9 96:16

elected
41:25

electronic
7:19 95:13

embodiment
32:13 33:10 35:11 36:3, 6 42:20 46:24,25 47:11 48:1 77:1,5,12 84:22 86:8 87:7 94:24 95:17

embodiments
28:23 31:2 32:19 34:5 44:10 46:4,5 51:22,23 52:8 53:7 58:5 95:18,24

employed
17:6,23

employee
17:24

empowered
82:14,19 83:3

enable
47:24

enabled
46:5

encompass
24:24

encompassed
48:23

encounter
27:8 65:3 70:1 81:14

encrypt
39:10,19 42:5,13 43:21 46:9 51:25 63:2,12 86:14,18,20

encrypted
22:8 24:3,24 26:20 39:4 40:4 42:15 43:2,4 44:3 46:20 47:10,13 83:20, 23 86:13,21,24 93:24 94:1

encrypting
31:8 39:18 42:21 62:16, 24 63:4

encryption
25:14 26:4 30:13 37:13 38:6,8 39:9,14,22,23,25 40:1,5,9,19 41:15,21,24 42:1,3 46:10,21 48:12, 16 50:9,14,20 52:1 61:13,22 62:6 63:3,6,23 80:8,15 82:11 83:11,15 86:7,9,12,25 87:3,5,7, 21 91:7,15 92:4,10,17 97:2,5

encryptions
62:8

encrypts
86:16

end
12:18 97:10

Endless
38:18

enforcement
83:4

engine
86:18

ensure
7:5 82:12

ensuring
19:14

entails
17:18

entire
31:18 38:14 39:19 95:21

entirety
27:6 64:24 69:24 81:12 94:13

entities
20:25 21:2,4,5 28:10,17 29:2,8,11 35:15 36:8,18 46:17 49:5,9,13,16 51:9,11,12,14,24 54:2, 18 55:13 56:7,12 57:19 59:16 82:14,19 83:3,6 88:1

entity
20:19,22,24 21:10 28:9, 16,24,25 29:5,16,18,24 30:3,4,16 32:9 47:1,22 48:3 49:25 51:19 52:16, 19 53:18,21 54:4,6,12 55:4 57:3,5,6,7,18 74:7 78:22 79:5,9 88:4

environments
77:11

equal
69:5

errors
14:16

escape
36:24

essentially
18:5 86:22 87:23

EST
90:14 97:16 98:14

estimate
13:4,6

evaluated
19:19

Evenhaim
10:1 26:23,25 27:3,6,8, 11,17,20,24 28:20,22, 24 29:25 30:9,23 31:4, 13,15 32:16,18,25 33:3 34:12 37:8,9,16 38:22 40:7 41:23 43:14 44:4, 6,8 45:25 46:4,8 47:20 48:10,16 49:9,12 51:22 53:4,12 54:1,9,17,25 56:4,6,11 58:2,6,7,16 61:8,18,25 62:3 63:24 69:20 73:3 79:12 93:4 96:24 97:3,7

Evenhaim's
50:8,10 56:1

Evenhaim/settimi
97:6

evidently
67:11

EXAMINATION
6:8

examining
66:2

examples
28:16 31:7,24 34:11,15, 25 53:12,25 54:24 58:22 73:19 74:1

excluded
16:10

Excuse
66:20

Exhibit
9:2,21 10:2,6,10,16 13:18 16:13 25:8 26:23 64:14 69:17 81:4 94:9

exhibits
9:16

exist
14:17 56:5 88:20

existed
39:2

expect
75:2,14,23

experience
13:25 21:5

expert
11:13 12:2,16 14:24

explain
27:20 62:20 67:4

explained
33:13 89:15

explaining
34:2

explains
66:25 89:20

explicit
55:16 59:22 69:1 75:22 77:16

explore
14:11

express
54:16 55:3,6,7,17 58:7, 16

expressly
54:8,24

extent
20:16 30:5 37:3 88:7

F

face
44:23

facets
47:24

facilitate
35:12

facilitated
48:13

fact
56:4 57:3

factor
15:23

factors
26:5,15

facts
40:16

fair
76:23

False
89:15

familiar
26:25 38:16 64:19 81:6, 17 94:11

feature
83:10

fed
39:15

feel
65:23

field
14:1 69:1 81:24 82:5

fields
40:23 43:4,10,12 51:3,6 55:14,20

figure
25:25 28:3,8,16 29:15 30:7,8 32:2,5 35:22,24 36:6,16 37:6 42:9,12 43:1,24 44:11,18 45:3 56:22 58:23 59:3 60:3 70:11,13,21 77:2,6,9,10 78:5 84:1,6,25 87:25 88:11,16 91:16 94:19, 22 95:1

figures
27:23,24 34:4,9

file
12:9 23:9 24:10,17 37:10,12 98:11

filtering
18:16

final
24:21 36:14 66:24,25 67:15 98:4,7

find
19:21 27:22 33:10,14, 18 68:25 77:15

finding
80:7

fine
33:24 45:15,18 64:7

firewall
78:12

Fish
6:12,15

fits
41:8

five-minute
45:14 64:5

fix
82:23

flows
88:19 89:4 93:19

focus
83:8,12

focused
40:4

focuses
53:5

folder
7:21 9:23

follow
93:6

force
26:22

forced
67:13

foregoing
24:23

form
28:11 30:17 35:3 39:22 44:21 47:3 52:22 63:8 66:12 78:18 93:10

format
73:7 75:4

formats
74:25

formatted
72:21,24

formatting
72:16 75:9,12,20

formed
22:17 48:20

forming
13:19,23

forward
62:9 73:8

forwards
78:8

found
33:15 56:8

Foundation
44:21 91:9

founded
19:8

free
65:23

front
12:13

fulfill
85:20

full
8:5

function
44:10,25 47:23 48:3 51:2 54:7,13,21 67:2,5, 12 71:9,20 92:15 96:3, 6,20

functionally
30:12

functions
32:23 33:12 34:7 47:5 48:20 50:21 70:24 71:23 72:4,11 76:23 77:13 85:20,22

G

gathering
50:6

Gaussian
67:1,5,12

gave
59:24

general
7:11 20:23 35:12 41:24 79:13

generally
37:17 42:24 51:13 70:13 80:19

generate
52:3 86:12

generated
24:4,5 58:12

generates
36:11

generating
86:19

generation
86:18

give
8:12 73:24

good
6:9 27:16 64:5 65:12 70:8 81:20 90:3 98:11

government
18:10

granularity
61:15

Great
9:25

greater
68:6 69:5,11

group
22:9 24:15 25:15,19 26:7,17 67:24

guarantees
20:15

guess
13:7 39:25 53:23 76:13

guidance
56:22

guide
17:8,12,20,22

Gupta
6:15

guys
21:6

H

happen
7:16 33:1,2

happy
65:16 90:8

harder
79:11

hash
26:1,3,6,8 80:7

hashed
26:12

hashes
38:12

health
28:5,15

healthcare
18:20 19:4,10 57:22,24 82:6 84:21

held
16:21

helpful
58:22

high-level
70:24 84:8

higher-level
72:23

HIPAA
18:14 19:14,18,22 20:11,14,20,25 21:2,5 29:6,8 30:4,16 48:9 49:24 50:1 51:12 56:23 57:4,11,18,25 59:19 60:4,6 62:17 74:7 80:25 88:1,4 92:16

HIPAA-COMPLIANT
19:1

HIPPA-COMPLIANT
18:12

history
12:9 23:10 24:10,18 60:20

hospital
29:1

hospitals
49:11

hour
7:11 15:17 45:12 90:8

hours
11:3 15:24 90:7 98:4

HP(I,J)
44:15 45:6,8

I

ID
32:3 47:16 83:20 86:13 93:24 94:1

idea
91:22

identifiable
29:3 57:12

identification
48:12 53:24 77:17

identified
11:8 13:23 17:10 67:24 74:3 83:13 84:24 85:2, 8,12,17 88:11,23 89:14, 18

identifier
22:25 44:15,19,24 45:2, 7,10 46:20 47:13 48:8

identifiers
44:1 45:9 47:10 48:5,6

identify

31:14 32:15 33:7 34:14 50:11 52:20 53:13 58:22 59:8,12

identifying
24:24 46:9 56:25

identities
52:9

identity
23:1 25:15,19 26:6,16 46:13 52:17 57:13

IDS
52:3 80:18

illustrates
77:10

imagine
58:13

immediately
14:6

implement
38:14 46:23 76:25 79:1, 4,8,14 80:11,22 82:11 88:10 91:7

implementation
18:12 19:1 31:21 36:23 39:6,24

implemented
32:11 87:19

implementing
42:8 64:2 78:13

import
96:3,6

important
29:10

impossible
11:14 12:5

Inc./paul
16:18

inclined
56:9

include
22:7 31:16 32:4 35:5 37:13,17 40:14 43:10, 12 56:24 60:15 74:1 80:14 92:10 96:11,13, 18

included
16:13 60:22

includes
30:13 31:25 39:11 42:4 43:18 59:18 72:7 84:13 87:15 89:14 93:24 96:2

including
35:1 41:15,25

incompatible
40:6

incorrect
23:5

index
9:18

indication
68:18

individual
22:25 23:1 46:12,13,21 47:9,12,19 48:12 50:11 52:21 53:10 57:14 59:6, 10 63:4 66:8,16 87:20

individual's
31:6 47:24 48:4,7

individually
22:23

individuals
20:15 25:15,19 26:7,16 29:12 41:25 42:4 48:13 52:10 59:13 66:16

Indranil
6:14

infeasible
25:21,23 26:9,11,22

inference
67:19

inferring
88:25 89:2

information
22:8 23:20 24:5,15,24 26:14,20 29:11 47:18 49:3 50:15 56:25 57:12, 13,24 58:3 59:5,6,15, 18,23 60:2,3,7,17,22 66:3 70:14,18,19 73:9, 10,13,17,20 74:4,6,9, 13,20 76:10 77:22 85:16,19 86:1 91:22 92:21 93:14,21,23 97:4

instance
41:18 82:24

institutions
21:8

instrument
17:19,21

insurance
21:7 50:5

intake
74:14

integrate
91:14

integrity
37:25 38:2,10

intent
38:23 86:8

inter
6:23 9:7

interest
21:9 59:9

interested
36:4

interesting
95:22

interface
36:10

interim
46:5

interior
40:3

internal
52:6

internet
71:5 78:11 81:2

interrupt
7:6

intranet
71:4 78:11

invention
9:13 56:1 81:25 82:4,5, 10 83:14

invite
31:23

involve
17:13

involved
15:8 18:11,15,20,25 19:14 27:13

involvement
27:12 65:7 70:6 81:18

involving
6:24 22:4

IPR
6:24 7:20 9:6,8 11:12, 17 27:12 81:18 94:16

IPRS
12:3 15:7

issue
17:16

items
40:23

J

January
17:25

Jeffrey
6:15

joined
6:14

July
16:22 17:25 21:25

Justin
6:19

K

Kerberos
14:5

key
39:9,12,14 46:10,21 47:23 48:2 52:1,12 82:11 83:20 86:14,16, 18,21,22,23 87:15,18 88:8,18

key-based
86:10

key-management
86:11

Keyed
38:12

keying
26:13

keys
42:6 61:14 83:17 86:20 87:21

kind
40:1

knowing
47:22,23 48:2

knowledge
16:3,6,9 80:9,25 94:15

L

labeled
9:23 10:8,12,13,18 85:7,8

laboratory
74:3

Landi
81:3,6,9,12,14,18,21,23 83:8,13 84:7 86:5,9 87:1 88:21 89:12 90:25 91:18,24,25 92:14 93:1, 2,14,23

Landi's
91:7 92:4,23

language
25:13

larger
20:2

law
29:13 49:4 83:3,4

layers
39:23

left-hand
29:19 66:19,24

legally
82:14,19 83:3

length
73:3

level
41:24 42:1,3,7 61:7,10, 17 62:4 86:15

levels
40:20 49:19 61:13

libraries
81:1

lieu
92:24

light
42:23

likewise
79:7

limitation
65:15 66:15 68:25

limiting
69:1,9

lines
37:8 40:7 41:22

link
46:11 47:8 53:9 57:23

linkage
47:22 48:3

linked
53:22

linking
96:18

list
13:18 15:2 19:21,24 31:17,25 32:3 34:25 35:10,14 41:25 42:4,13 43:7,23,25 44:2,15,19, 24 58:2,14 59:23 60:23

listed
20:8 74:5,15

lists
31:8,10,15 44:20 45:2,5

litigation
14:24 22:4

LLC
6:13 8:22 16:18 17:2

located
32:16 33:5,8,20 86:25

locations
48:11

long
25:24 65:1 92:19

longer
45:16 74:16 90:5

looked
12:11 65:1

lots
28:23 31:13 96:13

lunch
7:12 90:3,16

M

made
98:11

main
91:22

maintain
29:2 51:15 84:23 85:17

maintained
52:16 54:3

maintains
95:12

make
6:17 14:1 45:15 52:5 89:5 93:12 96:19

makes
36:13

management
39:12 52:12 88:18

manager
74:2

managers
28:5

mapping
97:5,7

maps
85:23

marked
9:1

Maryland
8:9

Massachusetts
22:5

master
87:15,18 88:8

match
24:6 43:4,20,22 47:16 53:13 54:2,7,13,20 63:2,11,17,21

matched
43:10,13 51:4,5,6 87:13

matching
30:13 50:11 51:24 52:2, 18 54:17 55:5 56:7,11 62:15

material
11:8

matter
22:16 23:6 24:2

matters
12:3 14:25 27:14

meaning
21:23 24:19 25:4

meaningful
51:3 73:4

means
25:24 26:22 52:7

mechanisms
80:5,20

medical
17:8,12,14,22 18:12,19 19:1 20:16 22:8 24:14 29:11 31:6,11,16 32:1,4 34:13 35:1,6 57:10,23 58:3,8,14 59:6,18,23 60:2,14,15,17,20,22 70:14,18 73:9,13,16,20 74:6,9,13,19,20 76:10 77:22 85:16 86:1 95:13

medication
59:13 60:6

medications
59:5,8 60:8

meeting
10:21

meetings
10:24

memory
13:13 23:19 56:13

mention
46:16

mentioned

74:24

merger
46:5 48:12,16

merging
96:11

message
38:13 39:4,18,20 40:1 63:6

method
77:11

methodologies
80:10,12,14,23

methodology
80:3

methods
79:17,21,23 82:10

microdata
29:3 34:23 35:5 36:20

mind
14:6 35:17

mining
21:9

minor
20:1

minutes
45:17 58:21 90:10 97:11

MIR
73:16 74:16 75:11,17, 20 76:1,9 77:2,6 78:2 85:19 92:25

modification
92:22

modified
38:4

modify
68:4 91:13

modifying
92:9

module
32:6,8,16,22 33:4,8,20 44:13,14

moment
50:6 65:22 73:24

money
21:6

months
13:10

morning
6:9,10

motivation
42:21

move
33:25 76:23 77:13

multiple
39:23 45:2 46:19 58:5 61:13 62:8 70:21 91:19

Murphy
10:15 64:13,19,21,24 65:3,7,13,18 66:1,4,25 67:8,17 68:3,10,11 69:3,12,20

Murphy's
66:9

N

named
20:3

names
57:9,14,19 58:25 62:17 63:5

nature
12:14 18:7

necessarily
14:21 30:3,15 32:23 34:7 39:21 43:3 46:22 56:3 60:16 67:16

needed
7:12 82:15

network
18:2 23:20 39:19 41:6, 10,17

networks
36:22

Nick
6:11

noncovered
57:5,7,18 78:22

noon
64:9

normal
15:17

notes
40:7 41:23 48:16 50:6

number
9:16 15:24 31:9 39:7 40:19 42:22 48:20 66:10 67:11,24 68:7,11, 12,15,17,21,23 69:2,4, 10,11,12,13 77:18 80:4 81:1 82:21

numbered
85:7

numbers
38:18

numerous
48:11

O

oath
8:10

obfuscate
66:5 67:6

obfuscated
67:23 68:6,11,12,15,17, 21,23 69:4,13

obfuscates
67:23

obfuscation
68:5

Object
35:3

Objection
28:11 30:17 40:16 44:21 47:3 52:22 63:8 66:12 91:9 93:10

occur
10:24 32:24 48:17 49:1 51:24 53:18 54:22 55:6 62:6 75:15,16

occurred
53:20

occurring
41:21

occurs
54:5 87:3

October
98:5,8

offer
67:21

offering
16:4

office
29:1 74:3,5

Oliver
6:19 28:11 30:17 40:16 44:21 47:3 52:22 63:8 66:12 91:9 93:10 97:24 98:10

one-way
26:1,4

operated
28:4,9 84:20

operations
17:3 36:16

opinion
16:4 22:17 23:7 42:18

opinions
12:17 13:20,24 14:7,12 16:7,10

option
71:4,5 92:9

options
71:3

order
24:12 31:3 43:21 51:2 54:20 56:23 63:2,17 83:5 98:3

ordinary
9:12 21:22 24:19

organizations
84:21

original
26:12

output
67:1,13,18,22

overview
84:6

owner
6:13 8:21

owners

82:13,18

owners'
22:4

P

p.m.
64:11 89:25 90:14 97:16 98:14

package
16:12

paper
19:21 20:4,7,9

paragraph
15:15 21:14,16,17 22:2 24:22 37:16 41:22 46:3 56:17,21 61:1,6,18 62:1,9,14 66:19,23 73:19 77:21 80:1 90:21, 24 91:5 92:3 96:9,10

parameter
41:25 42:4

parameters
66:11

part
32:8,22 34:8 58:25 59:7,23

partes
6:23 9:7

pass
97:23

passed
74:23

passing
85:19

past
15:10 36:24

patent
6:13,24 8:21,25 9:1,2 12:9 14:8 22:3,5 23:10, 14,24 24:8,10,25 25:7 26:19 61:7

path
93:6

patient
30:2 31:8,10,15,25 32:3 34:25 35:10,14 42:13 43:7,23 44:2,15,19,24 45:2,5,7,8,10 50:12 51:20 53:9,15 57:9,19 58:2,13 59:22 60:23 62:17 63:5 74:4 76:14 77:6,18 78:15 79:18 82:12,13,18 83:12 84:10,13,19,23,24 85:2, 6,8,12,15,17 86:5,6,13 87:1,6,9,10,11,22,24 88:3,12,22,23 89:13,14, 18,19 92:23 93:8 95:5, 10,15,19 96:8,11,12

patient's
34:13 52:17 60:14,20 83:19

patient-level
29:3 36:20

patients
31:16 43:25 51:15 58:3 59:5 60:7 66:10 67:24 82:15,20 83:9

patients'
31:11 32:1

Paul
6:3 8:7

PBM
28:15

PCP
95:12

PCPS
94:25 95:2,5,7,15

people
18:15 38:5 53:1

percentage
12:24

Perfect
98:9

perform
50:10

performed
33:12 48:20 54:17 92:17

performing
47:22 50:9

performs
48:3

periods
74:16

permit
53:9

person
9:12 18:5 42:25 47:15 54:14 60:5 79:22 80:11, 21,24 89:2,22

personally
56:25 57:12

perspective
19:6,23 32:4

pertain
47:15

pertains
55:25

Petitioner
6:17,20 8:17 22:20

pharma
21:8

pharmaceutical
28:4 29:14,17,20 36:7 37:5 58:23 59:4

pharmacy
74:2

phrase
9:6

physical
77:10

physician's
74:2,5

PII
18:21 19:5,11 20:17 29:7,22 30:6,19,21,24 31:2,5,9,22 32:19 33:11,18 34:6,12,21,24 35:5,21 36:13,24 37:4 48:8,25 49:7 51:15,25 53:5 55:14 57:6,8,9 63:12,22 66:17 67:19 74:8,11 76:15 79:16 80:18 85:14,24 86:16 88:2,7,15,19 89:5,16 92:19 93:1

PII-CONTAINING
91:23

place
32:11 47:4 92:4,15

places
33:1 48:21 50:5 53:6

plain
24:19

plan
28:15

plan/pharmacy
28:5

play
52:13

plug
91:18 92:7,14

plugging
91:25

plural
45:4

point
19:2 33:16,24 51:16 54:1,18 55:7 59:2 64:5 89:12

policy
18:15 19:16 40:24

portion
43:14 55:18 59:3

portions
12:19 40:3 46:9 56:6,11

POSA
9:11 21:24 24:22 56:22

POSITA
9:11 54:23 78:21

position
34:10

positions
16:21

possession
29:22

possibilities
31:13 51:22 69:14 76:18

possibility
58:20 68:1,13,24 69:12 76:19 77:20 78:23

potential
33:1

power
90:9

precluded
16:3

preferable
37:17 40:9,14 42:24

preferably
37:12

preferred
77:10,11

preparation
11:4

prepared
10:19 12:8

preparing
11:2 12:15 14:4 27:3 64:21 69:21 81:10

present
56:1 65:7 70:6 82:3,9

president
16:17

pretty
26:18 44:25 65:1

prevent
37:24 38:8 67:19

primarily
11:7 18:10

prior
10:22 55:25

privacy
19:14 20:11,14 47:25 48:4,7 50:1 55:14 82:6,12 83:12

privacy-identified
55:20

privacy-sensitive
34:22 35:4

private
29:11 86:23 87:15,18 88:8

problem
63:23 82:22

procedure
57:24 58:14

procedures
17:15

proceeding
6:24 9:2,7,8,21 12:8 27:4 65:8 69:22 70:6

proceedings
98:13

process
12:7 50:5 52:25 53:3 70:17

processed
33:18 35:1 79:16

processing
32:19 34:6 46:11 47:2 75:14,16 84:11,14,19,23 85:6,15 86:6,13 87:1,6,11,24 88:3,13,22 89:13,19 92:24 93:8 96:15

processor
23:19 25:14 48:17

processor's
48:18

produce
39:16 46:20 52:1 73:5 86:6

produced
93:21

produces
68:11,22 95:10

producing
25:10,11,13

products
17:15

projects
11:20 18:8,9

prompted
25:3

prop
17:1

proposed
92:4 93:16

proposing
91:6,13 92:23

protect
29:7 39:2 40:20 41:17 49:3 55:13

protected
60:6 85:14 92:19

protecting
19:5,11 83:12

protection
42:7 82:6

protections
60:4

protocol
38:25 39:11 51:7 72:22,25

protocols
38:20

provide
13:12 22:15 38:6,11,19,22 41:5 42:7,16,24 43:2 44:3 49:13 59:22 61:16 69:12 76:4,6,9

provided
9:24 12:11,17 13:18 14:5 20:17 23:12 27:10 36:10 65:5 66:5 70:3 76:15 81:16 94:17

providers
95:5

provision
49:24

provisions
57:4,17

pseudonyms
80:18

public
86:10,14,16,21,22 98:11

publication
19:20

publications
20:2

published
19:21

put
7:21 12:12 13:4 32:14

Q

queried
74:19 92:24

queries
39:2 43:17 50:25 51:3,8 66:15 71:11 87:12

query
36:11 41:18 42:13,15 43:1,3,8,9,12,15,16,17,19 51:18 54:20 55:5 56:23 58:12 59:1,7,8,14,17,23 60:9,11,13,19 66:1,2,6,9 67:25 69:4 72:16,20,21,24 73:4,7,8 74:18 75:1,4,9,17,20,25 76:5 78:4 93:2,5 97:4

querying
50:15,18 59:16

question
25:5 26:18 55:1 57:16 59:21 60:16,21 62:22 66:22 85:4 91:10 94:18

questioning
8:16 21:11

questions
7:7 27:21 65:16,21 69:19 91:3 97:12,22,25

quote
62:16

R

randomize
67:5,11,12,17,22

randomizing
66:25

range
67:1 68:4,6,18

rate
15:17,20

re-ask
91:10

re-encrypt
40:2

reaches
78:16

read
14:1,21 27:6 31:18 32:2 37:14 42:23 44:22,24 46:14 64:24 68:4,14 69:24 81:12

reader
80:9

reading
43:1 80:2

ready
64:3

reason
8:12 23:4 27:19

reasonable
65:14 76:16

reasons
79:6 82:21

recall
11:11,14,15 12:3 13:2 14:4 20:6 27:11,13 72:3,5 95:23,25

receipt
73:8

received
7:19 52:18 53:14 54:2 72:16

receives
49:25 52:10 74:25

receiving
37:11

recently
12:6

recess
45:20 64:11 90:14 97:16

recites
25:13

recognition
17:19

recollection
28:22 30:25 61:20 65:6 70:5 72:1 79:20 81:17

reconvene
64:8 90:11

record
7:5,18,20 8:6 9:18 18:13 19:1 34:1,2,4 46:9 52:16 83:19 98:2

records
20:16 26:25 32:3 46:11 47:8,13 50:12 53:9 60:14,19 66:14 69:2 82:13,15,19 95:13 96:12

recover
26:12

refer
9:16,20 10:1,5,9,15 25:7 46:17 61:6

reference
27:9 31:19 35:7 51:17 52:7,14 56:9 64:4,13 65:4 69:16 70:2 72:6 75:6 80:7,22 81:4,6,15 89:9 94:8,16 95:21,25

referenced
45:3

references
10:23 11:6 12:10,11

referred
43:23

referring
8:17,22 9:1,7,12,19,20 10:1,5,9,15 21:12 43:15 45:8 57:9 59:3 67:9 77:25

refers
40:12 43:16 46:4

reflects
32:13

regard
38:10

regulations
21:1

reidentification
83:9,13,16,18

reidentify
82:14,20 83:7 87:22

related
21:20 46:12 47:9

relates
82:4

relation
18:22

relax
34:18

release
29:11 76:15 95:15,20

released
78:1 87:9,11

relevant
17:11

rely
97:1

remedied
14:22

remember
75:22

repeated
62:16,23 63:3,23 66:15

repeatedly
63:2

rephrase
57:16

replace
91:21

replacing
91:23

report
95:10

reporter
16:1 40:17 77:3 83:22 96:21 98:1,6,9

repository
73:10,17,20 74:6,14,21 77:22 85:12,16 86:2 88:12

representations
28:3,8

represented
85:25

request
36:9 63:5 66:11 71:13, 17,22 72:19,22,23 73:8 74:25 75:4,9 92:13 93:13

requested
16:1 40:17 77:3 83:22 96:21

requester
36:15 37:3,5

requester's
71:13,15,18,20,24 75:19 78:7,8,16 79:5 91:8,14,21 92:5,13,18 93:7,18 94:2

requesting
59:4 70:14,25 71:9,12 72:17 78:1,9,21 79:1 93:11,17 94:2

requests
23:21 70:17,19 72:16 98:2

require
34:7 41:7 60:4

required
67:16

requirements
49:20,22 61:23

requires
41:9,11

requiring
37:9,11

reread
10:22

research
11:19 21:8

residence
8:8

respect
22:3 24:14 69:20

respective
34:22 37:11,13

response
23:20 27:21 67:25 69:3 70:19 76:4,9 78:4 93:6, 16

responsibilities
16:24 18:4

responsible
12:22 17:2 29:5 72:15

restart
66:22

result
66:9 67:23 68:22 76:1

results
36:12 41:19 66:5 67:6, 21 73:5

retained
14:24

retrieving
70:14

return
53:8 66:14 67:20 70:18 76:1 77:22 92:20 97:14

returned
69:2

returning
40:8 68:6

returns
68:18 69:3 77:6

reveal
23:1

reversible
83:11,15

review
6:23 9:7 11:4 22:11 24:8,17 27:3 31:23 64:21 65:23 69:21 81:9 95:21

reviewed
11:9 12:9 23:9 94:13

reviewing
14:4

Richardson
6:12,16

right-hand
68:2

Rishi
6:15

role
18:4 52:13

roles
16:25

rough
98:4,5

routed
71:15,17 78:4 93:3,13, 17 94:2

routes
71:22

routing
91:22 92:13

rule
19:15 20:11,14 50:2

ruled
52:7

run
17:1

S

S-HTTP
38:20

S/mime
38:20

Sarkar
6:14

satisfy
66:10 93:14

scanned
64:25

schematic
42:20

scheme
39:9 52:12

schemes
38:15,17 40:19 41:3

scientist
18:1

scope
26:19

scroll
73:22

search
30:1 35:20 55:10 56:9 58:19 66:11 72:1 79:19, 24

searched
58:10

searching
35:12 75:13

section
21:19 66:4 81:24 82:3

secure
18:16 34:20,21 40:22, 23,24 41:14,16 49:8

secured
35:21 82:11

Securemethods
16:18 19:4,7,8,10

securing
53:5

security
19:18 36:25 37:1,2,18, 21,23 38:7,11,17,19,22 39:5 40:15,21 41:4,5,10 42:16,25 43:2 44:3 47:6 48:21,22,24 49:6,18,19, 20,22 52:25 61:7,11,17 62:4 63:7

security-related
18:9

seek
36:24

seeking
67:19 68:25

select
43:18

send
35:14 41:6,10 59:15

sending
37:4 53:21

sends
36:9,14 75:25

sensitive
18:17 35:13 37:4

sentence
56:21 68:16

separately
44:19

separation
53:1,3

September
6:1

series
35:23

served
11:12

server
22:7 23:18,24 25:14 30:12 31:21 36:9,10,11 37:2 41:14 59:14 71:14, 16,18,21,22,24 72:8,11, 12,15 73:4,7 74:15,19, 24 75:8,19,25 76:2,7,10 77:7 78:7,8,12,16 79:5, 8,11 88:8 89:5 91:7,8, 14,15,20,21 92:5,8,10, 13,17,18 93:7,18 94:3 97:2,5

servers
76:24 85:24

set
42:13 52:24 84:10

Settimi
10:5 94:8,11,16,20 96:23 97:1

shorthand
73:12

showing
58:23 72:10

shown
28:16 30:7 32:5 34:9 35:23 36:6,16 71:7 77:1 84:25 88:11,16,17 94:22,25

shows
28:3,8 84:10

shut
8:1

sic
66:23,24

side
29:19 47:6 48:17,18,21, 22,23 55:4 63:19 66:19 68:2 75:10

signed
78:18

similar
52:3 73:2 93:6

similarly
14:19 22:8 24:3,14 73:16 79:3

simply

23:7 63:4

single
55:21 66:16

sir
8:4

sit
34:18 58:18

sites
84:20 96:8

sitting
11:11 72:3 95:23

situation
41:20 58:13,17

size
41:8

skill
9:12 31:20 40:25 42:25 54:10,14 79:22 80:11, 21,24 89:10,22

slightly
24:1

sole
17:1

solution
66:24,25 67:15

solutions
18:2 67:20

sort
51:16 70:23 75:12

sorts
37:25 38:20 39:12 96:15

sought
59:19 60:18

source
28:10,16,24 29:2,5,11 32:9 35:15 36:18 46:17 49:12,16 51:8,11,14,24 52:16,19 53:18,21 54:1, 3,5,12,17 55:4,13 56:7, 12 57:3 60:11 62:6

source-entity
48:18

sources
34:21 46:8,16,20 49:1 50:10 51:6,25 52:6,9 53:8,13 56:24 58:2,9 73:11 93:2

speaking
7:6 51:13 80:19

Special
47:21

specific
14:3 20:21 34:11,14 40:23 53:12,25 54:24 57:20 79:20

specifically
18:19,22 43:8 63:25 68:14

specification
23:9 24:9,17 31:23

spend
11:1

SQL
43:18

SSL
38:18 39:2

SSL-LEVEL
40:5

stake
21:8

standard
38:24 43:17

start
34:19

starting
46:7 55:12 82:8

starts
21:19

state
8:5,8 21:22

stated
14:12 24:25

statement
62:20

step
25:10 37:9,11 42:12,16 43:24

Stephens
6:8,11,22 16:2 28:14 30:22 35:3,8 41:2 45:1, 11,17,19,21 47:7 53:2 63:14 64:3,8,12 66:18 77:4 83:25 89:25 90:10, 13,15 91:12 93:15 96:22 97:9,14,17,22 98:3,7

steps
35:23 36:2

stored
60:11

stores
74:3

storing
54:11,19 63:20

stream
39:16

streaming
40:5

streaming-level
38:19

string
39:15

stronger
42:1,3

strongly
41:23

structure
96:14

stuff
12:17,18

subject
20:25 35:6 50:1 82:14

submit
71:13

submitted
14:14

submitting
71:11

substance
45:23 90:19 97:20

suite
17:15

super
39:22,25 41:21 61:22

support
77:21

supported
56:4

supports
50:9

surveillance
84:16 87:14

sworn
6:4

symmetric
86:19 87:20

system
18:13 19:2 30:7 42:12 43:5 49:2 51:2 52:24 54:7,21 61:15,23 64:2 70:13,17,22 72:7 73:9, 14 74:10,13,20 75:3,16 76:22 78:13 79:1,4,8,15 84:7,13,14,16 86:7,9, 11,12 87:11,14 88:4,13, 23 89:13,19 91:24 92:4, 14,16,23,24 93:8,13 95:8,20 96:2,20

systems
24:12 28:4,9 39:22 42:8 52:4 56:3 75:15 76:25 82:10 84:11,19,23 85:6, 15 86:6,13,25 87:1,5,6, 8,24

T

table
13:23

taking
6:12 60:5,8

talk
36:5

talking
26:19 29:17 73:6 88:7

talks
34:6 55:19

target
17:21

targeting
17:20

team
97:12

technical
18:5 19:6,16,22 81:24

techniques
80:16

technology
27:17,20 65:13 70:9 81:21

telling
32:25 77:14 89:3,21

tells
29:13 69:9

ten
15:3,9 45:17 64:7 97:11

term
8:25 21:10 23:24 24:17 43:16 63:11

term's
21:22

terms
8:15,17,21 22:3,7,11 38:3

testified
6:6

testimony
8:13 45:23 90:19 97:20

text
34:5,9 39:17 89:12,17

things
28:12 33:1 37:25 39:12 41:11 42:5,22 43:18 49:11 53:1 61:22 70:20 72:18 80:14 96:13,18, 19

thinking
79:25

Thursday
6:1

time
7:10 8:3 9:13 11:1 14:13 15:16 39:20 55:2 63:1 74:16 90:3

timeframe
13:11 17:7

times
14:23 15:1,4,5,6,12 42:6 55:2

titled
81:24

today
6:13,23 8:10,13,16 21:11

today's
10:20 11:9

token
22:7,24 23:13 24:23 25:2,4 26:2 30:13 50:11 51:24 52:17,18,20 54:2, 3 55:15,17,19,21,23,24 57:2 62:15 63:1,11 91:17,24

tokenization
54:5

tokens
24:4 25:14,16,20 26:17 31:1,3 35:19,20 52:2, 10,15 53:8,14,22 54:11 55:4 61:14 63:11,20

tool
66:1,2,6,9

top
44:14 87:25

total
71:25 72:5 95:25

transcribed
7:3

transcript
98:1

transition
64:4

transmission
37:18,21,23 38:7,11,16, 22 39:5,19 41:4 42:16, 25 43:2 44:3 63:7

transmit
58:2 60:17

transmitted
36:17,21 58:15 74:18

transmitting
37:10 57:5,19 58:8

true
58:18 67:24

trusted
79:13

truth
6:5,6

truthful
8:13

turn
21:14 26:23 27:23 35:22 45:25 56:14 64:13 65:17 69:16 70:11 81:3 84:1 90:21 94:8

type
60:3 75:12

types
21:4 80:18 93:12

typically
39:4,8 49:11

typos
14:19,21

U

U.S.
6:24 9:2

unable
89:12

unattainable
25:15,20 26:7,17,21

unauthorized
37:24 38:1,4,8

unclear
91:11

understand
6:25 7:2 8:10,19,23 9:4, 9,14,22 10:3,7,11,17 16:17 18:1 20:19 21:11, 24 24:23 26:20 28:15 31:20 34:3 35:5 43:1,25 46:19 54:23 55:21 56:22 59:25 60:24 62:7, 22 63:11 64:2 69:7,8 73:12 78:6,21 85:4,13 89:11,22,23 91:6

understanding
20:10,13,23 21:24 23:24 24:16 27:16 29:9 35:9 36:1 37:20 43:9,15 44:8 45:6 50:7,10 55:23 65:12,14 67:8 68:10 70:9 81:21 91:4

understands
88:17 89:23

undo
82:22

unit
55:21

user
36:9

V

values
68:5

variety
88:9

Venable
6:19 11:23,24 12:1

versed
89:3

view
25:18 50:8

viewing
71:1,10,12 72:17 78:22

Vigilytics
6:13 8:22

violate
57:23

violated
57:5,18

violation
57:25

violations
37:25 38:2

virtue
88:19

vitae
16:14

W

waiting

33:14

wanted
50:16

warehouse
95:8,16,20 96:2

water
66:21

ways
25:1 35:17 38:14,20 39:7 40:20 41:15 49:15 53:6 57:15 67:11 88:10 91:19

week
10:24

wider
68:4

window
7:25 8:3

word
55:19,22

work
12:1,16 15:22,24 17:12, 17 18:19,23 19:13 24:12,13 54:6 75:2,24 78:14 86:9 90:9 92:8 94:16

worked
11:22,24 12:5 17:4 18:8

working
13:8

works
92:12

wrap
90:8

written
12:20 34:5

wrote
12:17,18

Y

years
15:3 17:9