Planet Depos®
We Make It Happen™

Transcript of Aviel D. Rubin, Ph.D.

Date: February 17, 2025
Case: Datavant, Inc. -v- Vigilytics LLC (PTAB)

Planet Depos
Phone: 888.433.3767 | **Email:** transcripts@planetdepos.com
www.planetdepos.com
Michigan #8598 | Nevada #089F | New Mexico #566

WORLDWIDE COURT REPORTING & LITIGATION TECHNOLOGY

1 UNITED STATES PATENT AND TRADEMARK OFFICE

2 _____

3 BEFORE THE PATENT TRIAL AND APPEAL BOARD

4 _____

5 DATAVANT, INC.,

6 Petitioner,

7 v.

8 VIGILYTICS LLC,

9 Patent Owner.

10 _____

11 IPR2024-00311, IPR2024-00381, & IPR2024-00382

12 Patent Nos. 9,965,651, 10,109,375,

13 10,886,012 and 9,665,685

14 _____

15 Deposition of AVIEL D. RUBIN, Ph.D.

16 Conducted Virtually

17 Monday, February 17, 2025

18 9:30 a.m. EST

19

20 Job No.: 571619

21 Pages 1 - 93

22 Reported by: Debra A. Whitehead

1 Deposition of AVIEL D. RUBIN, Ph.D., conducted
2 virtually.
3
4
5 Pursuant to notice, before Debra Ann Whitehead,
6 E-Notary Public in and for the Commonwealth of
7 Virginia.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

1 A P P E A R A N C E S
2 ON BEHALF OF PETITIONER:
3 JUSTIN J. OLIVER, ESQUIRE
4 VENABLE LLP
5 600 Massachusetts Avenue, NW
6 Washington, DC 20001
7 (202) 344-4000
8
9 ON BEHALF OF PATENT OWNER:
10 NICHOLAS W. STEPHENS, ESQUIRE
11 FISH & RICHARDSON, PC
12 RBC Plaza
13 60 South 6th Street
14 Suite 3200
15 Minneapolis, Minnesota 55402
16 (612) 355-5070
17
18
19
20
21
22

C O N T E N T S

EXAMINATION OF AVIEL D. RUBIN, Ph.D. PAGE
By Mr. Oliver 5
By Mr. Stephens 73

EXHIBITS MARKED IN TODAY'S SESSION

(None)

EXHIBITS MARKED IN PRIOR SESSIONS

(Not attached)

DEPOSITION EXHIBIT PAGE
Exhibit 1005 37
Exhibit 1009 48
Exhibit 2001 8
Exhibit 2006 19

1 P R O C E E D I N G S
2 AVIEL D. RUBIN, Ph.D.,
3 having been duly sworn, testified as follows:
4 EXAMINATION BY COUNSEL FOR PETITIONER
5 BY MR. OLIVER:
6 Q Good morning, Dr. Rubin. How are you?
7 A Good morning. I'm fine. How are you?
8 Q Fine, thank you. I'm just going to go
9 through a little administrative things first.
10 Is there any reason you cannot give
11 truthful testimony today?
12 A No.
13 Q You're not taking any medication that
14 would affect your ability to give truthful
15 testimony?
16 A No.
17 Q As you know since we've done this before,
18 I will endeavor to take a break about every hour
19 or so. If at some point you need a break before I
20 have called for one, please let me know. All I
21 ask is that you answer any pending question before
22 we take a break.

1 Is that all right?
2 A Yes.
3 Q And you understand that your attorney may
4 object to questions, but absent an assertion of
5 privilege you are still required to answer the
6 questions posed. Correct?
7 A Yes.
8 Q I'll try to be clear in my questions.
9 That doesn't always happen. If there's any reason
10 that you don't understand a question that I've
11 asked please let me know, and I'll try and make it
12 more clear.
13 A Okay.
14 Q I'll often be asking questions today
15 relative to the perspective of the person of
16 ordinary skill in the art. And I believe you're
17 familiar with that concept. Correct?
18 A Yes.
19 Q For simplicity sake, I will likely refer
20 to the person of ordinary skill in the art as the
21 POSA, just the acronym P-O-S-A.
22 Is that all right with you?

1 A Yes.
2 Q Great. Absent me specifying otherwise,
3 please use the POSA's perspective in answering my
4 questions.
5 How did you prepare for this deposition?
6 A I reread my reports and the patent -- the
7 patents and the prior art references, and I had a
8 couple of meetings with counsel.
9 Q About how many meetings with counsel did
10 you have?
11 A Two.
12 Q Two. Do you have any notes with you?
13 A No.
14 Q Are you emailing, texting, or otherwise
15 in contact with anyone else during the course of
16 this deposition?
17 A No.
18 Q I have uploaded and we can provide a link
19 to for exhibits, but, you know, if you already
20 have certain documents in front of you, that would
21 be easier, that's fine with me. So why don't you
22 let me know what you have before you before we go

1 through the whole downloading process.
2 A Sure. I have open my report on the '012
3 patent, but I have access to all the others. I
4 have Settimi, Evenheim, Landi open. I have the
5 '012 and the '651 patents open, but I also have a
6 folder with other patents and other reports if I
7 need them.
8 Q Great. Well, we'll go with the copies
9 you have for now. And if we need to transfer
10 anything to you, we will.
11 Just if you would confirm that the
12 versions you're looking at don't have any markings
13 or notes or highlighting.
14 Is that correct?
15 A Yes.
16 Q In that case, can you open your
17 declaration, Exhibit 2001 for the '651 patent,
18 which is for IPR2024-00307.
19 A Just a second. Let me find that.
20 (Exhibit 2001, previously marked, not
21 attached.)
22 A Okay, that's open.

1 Q And if you go to Paragraph 54 of your
2 declaration.
3 A Okay.
4 Q And if you look at the last sentence of
5 Paragraph 4 of your declaration --
6 A Oh, I thought you said 54. I'm sorry.
7 Q I'm sorry, I did say 54, 54 of your
8 declaration.
9 A Okay.
10 Q The last sentence says, "Although
11 tokenized health data has been used for other
12 purposes prior to the '651 patent, it has not been
13 used in the particular context or manner described
14 in the '651 patent."
15 Do you see that?
16 A Yes.
17 Q And what do you mean by "tokenized health
18 data has been used before"?
19 A The concept of replacing personally
20 identifiable information with a token was known.
21 Q All right. And what were some of the
22 contexts in which that was used or known in the

1 past?
2 A I'm not sure specifically, but it had to
3 do with anonymizing the data, or deidentifying it.
4 Q And just so we're clear on the term
5 "tokenizing healthcare data," I think you
6 mentioned that personally identifying information
7 was removed.
8 In that usage before, what would a POSA
9 typically do to tokenize healthcare data? And
10 I'll be more specific.
11 What is converted into a token and what
12 remains from -- relative to the original record?
13 A I'm not sure specifically. If you show
14 me a reference, I could discuss it.
15 Q Well, I'm just asking you what the
16 understanding of tokenizing healthcare data meant?
17 A Replacing identifying information with a
18 token.
19 Q And by "identifying information," that's
20 information that would identify the particular
21 patient at issue?
22 A Right.

1 Q So that could be a name or Social
2 Security number or address or something similar.
3 Correct?
4 A Yes.
5 Q So what information of the record would
6 typically remain after tokenization?
7 A I guess it depends on the hypothetical or
8 on the specific example that you have in mind. If
9 whatever was there that you didn't tokenize I
10 suppose would remain.
11 Q So if the example was a person's
12 healthcare record from a particular doctor's
13 office, would what remains after tokenization be
14 the specifics of the diagnoses and other details
15 relating to the medical treatment received?
16 A It depends on what was done, what that
17 particular system did to tokenize.
18 Q But generally speaking, tokenization of
19 healthcare data generally involved removing
20 information that would identify the patient.
21 Correct?
22 A That's my understanding of what could

1 have been done with tokenization.
2 Q Can you turn to Paragraph 70 of your
3 declaration.
4 A Okay.
5 Q And in the second sentence of Paragraph
6 70 you say, "In my analysis here I use the same
7 constructions relied upon by the petitioner."
8 Do you see that?
9 A Yeah, "relied on."
10 Q Yeah. So just for clarity, you're not
11 offering any alternative constructions for the
12 terms listed in Paragraph 70. Correct?
13 A Correct.
14 Q In that chart of claim terms from
15 Paragraph 70, or in Paragraph 70, the fourth one
16 down is similarly encrypted.
17 Do you see that?
18 A Yes.
19 Q And what would be a POSA's general
20 understanding of encryption?
21 A Are you asking me within the context of
22 this patent or just out in the world outside of

1 this case?
2 Q Well, why don't you answer both, and to
3 the extent that there's a difference.
4 A Yeah. So as we can see from the
5 construction, generated such that tokens generated
6 from corresponding information can be compared to
7 one another to detect a match, so that is -- the
8 idea there is that if you have a function that can
9 allow you to compare things, then that satisfies
10 similarly encrypted. So that could be, for
11 example, a hash function.
12 In the world outside of this case where
13 we're not using the context of any patent,
14 encryption has to do with making information
15 unreadable to anyone other than someone who has
16 the key.
17 Q Do you understand the patents at issue
18 here to be using the term "encryption" in a manner
19 contrary to the regular understanding of the term
20 "encryption"?
21 A Yes. In the patents in this case there's
22 a construction that both sides are using for

1 encryption, and it has to do with being able to
2 compare things to each other. And also within the
3 patents in this case you actually do not include
4 the ability to reverse the encryption function;
5 whereas outside of this case an encryption
6 function would have the ability to be reversed.
7 Q Are you aware of anyplace in the patents
8 at issue where there's a specific definition of
9 encryption given?
10 A I'm going to look at the patent.
11 Q And for ease of our discussion here
12 today, if you could use the '651 patent as the
13 example so that we're just being consistent when
14 we refer to --
15 A Right. That's the one I opened up.
16 Q Great.
17 A There are several discussions I think
18 that led to the definition that's being used in
19 this case. These have to do with descriptions of
20 the functionality of the encryption server, as
21 well as Column 7 at the top where it says, "To
22 produce tokens and request tokens, one or more

1 encryption techniques may be utilized, for
2 example, hash functions and other methodologies
3 may be implemented."
4 Q Well, sticking with the Column 7 language
5 that you just pointed out, that simply refers to
6 one or more encryption techniques. Correct?
7 A Yes.
8 Q And hash functions are just offered as
9 one example.
10 Is that correct?
11 A Yes.
12 I should add that the word "encryption"
13 in this patent is used in two different ways. One
14 of them has to do with the functionality of an
15 encryption server, which is to create tokens. And
16 the other is, if you look in Column 7, for example
17 Line 35, it's talking about encryption for sending
18 a request message.
19 And in that context it's talking about
20 the generally understood type of encryption;
21 whereas when it's talking about the functionality
22 of the encryption server that encrypts information

1 into tokens, that's using the definition that was
2 provided in this case. That does not involve
3 reversible function; it just has to do with the
4 ability to compare.
5 Q So I'm sorry, Column 7, what you pointed
6 out was Lines 35 through 43. Is that right?
7 A Yes. So it says, The request message may
8 be encrypted prior to being transmitted over a
9 computer network. The request message is
10 unencrypted.
11 So this is a different type of -- its's
12 using the same word "encryption," but it is a
13 different function than the one that's described
14 earlier where it talks about creating tokens.
15 Q And the place earlier where it talks
16 about creating tokens is what we just talked about
17 at the top of Column 7, Lines 2-5?
18 A Well, also, if you look at Column 6, like
19 around 54, "Each token obtained from the source
20 sites may have been created using the same token
21 generator used by the encryption server or using
22 any other means that generates the identical token

1 for the same personally identifiable information."
2 That is a different type of encryption
3 than the transmission -- than encrypting for
4 transmission.
5 Q And -- well, I'll come back to that.
6 Is there any place in the patent where
7 the term "encryption" is defined in two different
8 ways, one for the tokenization and one for
9 transmission? For instance, there any place in
10 the patent that says, For encryption I mean, and
11 then there is a definition given?
12 A It's going to take me a moment, because a
13 question like is there anywhere in the patent that
14 X occurs, I have to look at the whole patent.
15 Q Well, let me -- I'll rephrase it.
16 Are you aware in your preparation today
17 of any place that you already saw that has such a
18 specific definition?
19 A I think that, you know, when there's a
20 construction being used by the parties, then that
21 is a definition that's given. And I'm not aware
22 of anywhere in the patent that has the words, you

1 know, Encryption means X, and defines it that way.
2 But I think it's pretty clear from the
3 two different uses of encryption that that's what
4 is the case in the patent.
5 Q Can one create a token using the same
6 type of encryption technique that would be used to
7 encrypt a message for transmission?
8 A Can I please hear that repeated.
9 Q Sure. Could one -- could a POSA use the
10 same type of encryption that's used for message
11 transmission to form a token?
12 A No.
13 MR. STEPHENS: Objection. Form. Scope.
14 Q And are you talking about within the
15 context of this patent or just anywhere in the
16 field?
17 A In this patent.
18 Q Talking about generally in the field, if
19 one says encryption for data transmission, could a
20 similar encryption technique be used to tokenize
21 data just in the field of cryptography?
22 A I think it depends on whether you're

1 operating in a regulated environment like HIPAA.
2 HIPAA does not allow for reversible encryption of
3 tokens. So if you're asking could you program a
4 computer to do it, you could do that. But it
5 wouldn't be -- if you were working in a domain
6 that required compliance with HIPAA, then no.
7 Q With respect to your mention of within
8 HIPAA, what specific regulation are you relying
9 upon for the idea that only certain types of
10 encryption can be used?
11 A So I don't have handy, but if you have to
12 share with me the HIPAA privacy rule, I could show
13 you.
14 Q Okay. I'm going to put the -- I'll put
15 that document, again just put it in the chat and
16 you can download it.
17 A Yeah, that's easiest.
18 Q So I'm putting in the chat Exhibit 2006.
19 (Exhibit 2006, previously marked, not
20 attached.)
21 A Okay, I've got it. I just need a moment
22 to look through it.

1 So if you look at Page 2, under C.
2 Q Uh-huh.
3 A It says that, "A covered entity may
4 assign a code or other means of record
5 identification to allow information deidentified
6 under this section to be reidentified by the
7 covered entity provided that," and then 1 it says,
8 "The code or other means of record identification
9 is not derived from or related to information
10 about the individual."
11 And so that if you use information about
12 the individual to create the token, then this
13 would not qualify. And also the last part of 2,
14 says that it does not disclose the mechanism for
15 reidentification.
16 And so if the code is reversible, then
17 that would allow for reidentification. So I'm
18 relying on the Section C of the privacy rule.
19 Q Under C.2 that you just mentioned, The
20 covered entity does not use or disclose the code
21 or other means of record identification, in a
22 reversible encryption system where there is a key

1 that can decrypt, would the key that decrypts be
2 the code or other means to reidentify the
3 information?
4 A One more time, please?
5 Q Sure. In a public/private key system,
6 you can use one key to encrypt information.
7 Correct?
8 A Right.
9 Q And then there's a second key that's kept
10 private, in theory, that can be used to decrypt
11 that information. Correct?
12 A Yes.
13 Q And in that system is the private key a
14 means of reidentifying or decrypting information?
15 A I haven't considered that question. But
16 I'm also relying here on the second part, which
17 says, And does not disclose the mechanism for
18 reidentification.
19 And so using that other key would be the
20 mechanism for reidentification.
21 Q But that second part does not disclose.
22 That would only mean if you disclosed the private

1 key. Correct?
2 What if the private key was never
3 disclosed?
4 MR. STEPHENS: Objection. Form.
5 A So the key itself is not the mechanism;
6 the decryption function is the mechanism.
7 Q So let me ask this: If a doctor's office
8 uses the most up-to-date secure encryption method
9 possible to encrypt patient-identifying
10 information and releases a record with that
11 encrypted patient-identifying information, could
12 someone else reidentify the patient without having
13 the key, within reason?
14 A I think there are techniques used by the
15 NSA, such as TEMPEST and others, that could
16 interfere with that. But the mere possibility of
17 doing a decryption with the key is what makes
18 the -- this type of tokenization not HIPAA
19 compliant.
20 Q Why do you say "the mere possibility"?
21 A Well, in Rule 1 it talks about the
22 derivation, that the key is derived from the

1 information. So that would be one. And the other
2 is that there is a capability of reidentification.
3 So when it says, you know, it does not disclose
4 the mechanism for reidentification, that has to do
5 with the possibility of reidentification.
6 So my understanding of HIPAA is that if
7 you are able to reidentify, to reverse the process
8 of tokenization, then it doesn't matter if you do
9 it or if you have the key, that is not compliant
10 with the standard.
11 Q Well, it says, so long as you do not
12 disclose the mechanism for reidentification. I
13 mean, if no one -- if the person never discloses
14 the key for decryption, why would that be
15 problematic?
16 A Because, one, the key exists and it could
17 be found out. Two, the encryption might get
18 broken.
19 The idea behind this rule is to allow for
20 comparisons but not to allow for recovery of the
21 information from the token.
22 Q So why would you even -- why would one

1 even need to have, so long as they do not disclose
2 the mechanism for reidentification, if under your
3 interpretation the mere fact that it could be
4 reidentified is prohibited? That would seem to
5 render that language superfluous.
6 A I don't see the language you're referring
7 to. I don't see "so long as" in the language
8 here.
9 Q Sorry. It says, C.2, "and does not
10 disclose the mechanism for reidentification."
11 If the mechanism exists, doesn't that
12 assume that the mechanism exists?
13 A I'm not sure.
14 Q Let me ask another question, then.
15 If someone uses the most, you know,
16 robust public-private key system that they can and
17 they don't disclose the key for decryption to
18 anyone, would you agree that the risk would be
19 very small that someone could break the decryption
20 technique?
21 A And just to be clear, we're only
22 discussing 2 and not 1 in this example. Right?

1 Because you are assuming that the token is derived
2 from the user identifying information.
3 Q Correct. I'm just talking about 2 now.
4 A Okay. So I think the answer is, it
5 depends. It depends on the security posture, on
6 the random number generation source, on the lack
7 of a targeted adversary.
8 So, I mean, there are cases where data
9 can be protected by parties. But I think the
10 reason for these rules is that there are a lot of
11 times -- and I've seen it in my consulting
12 business -- that someone thinks that they've
13 protected information but they actually didn't do
14 a great job of it.
15 Q But if they did do a great job and they
16 did use a good encryption system and they did keep
17 the key secret, then they could make it so that
18 the risk is very small?
19 A I don't think you could say that in a
20 general context as that which must be considered
21 by someone writing a standard.
22 But I agree that there are organizations

1 that have more capability in security than others.
2 And so if you're asking me is it possible for the
3 most well-funded, you know, best-positioned entity
4 to do something securely, I think they can do
5 better than others. But I don't think anything is
6 perfectly secured.
7 Q Going back to what you pointed out, C.1
8 of the HIPAA privacy rules. The code or other
9 means of record identification is not derived from
10 or related to information about the individual.
11 Let's take the example of -- let's
12 actually look at the '651 patent.
13 A Okay.
14 Q If you look at Column 2 of the '651
15 patent, at Lines 44 to 46.
16 A Okay.
17 Q And that states that the request token
18 for each individual may represent encrypted data
19 that identifies the corresponding individual.
20 Correct?
21 A Yes.
22 Q So that's indicating that the token

1 that's formed is encrypted information about the
2 identify of the individual. Correct?
3 A Well, it represents it.
4 Q Is your understanding the '651 patent
5 that the tokenization takes a personal information
6 about the individual and encrypts it using some
7 method, for instance, a hash function?
8 A Yes.
9 Q So in that way, the token created in the
10 '651 patent is derived from information about the
11 individual. Correct?
12 A Right. So I see the tension here. And I
13 think to answer that, we can look back at Section
14 C of the rule.
15 Q Okay.
16 A And it says that, "A covered entity may
17 assign a code or other means of record
18 identification to allow information deidentified
19 under this section to be reidentified by the
20 covered entity provided that," and then 1 and 2.
21 So if there is no mechanism for
22 reidentifying at all, if that's not possible like

1 in the event of a hash function, then this
2 wouldn't apply.
3 Q That sort of brings us back to 2 then,
4 and says, "And does not disclose the mechanism for
5 reidentification."
6 Why would the rule need to say anything
7 about disclosing the mechanism for
8 reidentification if under your interpretation it
9 can't exist?
10 A So when -- so Rule C applies in the
11 instance where reidentification is possible. And
12 so under 2, it says it doesn't disclose the
13 mechanism for reidentification. I'm not sure I
14 understand what the problem that you're suggesting
15 is.
16 Q Well, let me ask this: This Part C
17 assumes or provides the manner of allowing for
18 reidentification. How would one reidentify the
19 individual using a hash function if they had
20 encrypted using a hash function?
21 A You can't.
22 Q What about the doctor's office that

1 creates the hash function? Don't they know what
2 the hash was, relative to the name they put in?
3 A They don't need to recreate the hash
4 function because they have the original.
5 Q But they would be able to correlate the
6 two?
7 A They have it all together because they're
8 the ones that made the hash.
9 Q Just for clarity, a hash function that
10 we're discussing about for tokenization would
11 take, for instance, some identifying information
12 about the individual, such as their name, and
13 basically convert that information into the
14 resulting token. Correct?
15 A That's one way to describe it.
16 Q So it's essentially a reconstituted form
17 of the input?
18 A I'm not sure all cryptographers would
19 agree with that, but I see what you mean by that.
20 Q And the reason I'm saying that is because
21 the hash function is reproducible. Meaning if
22 anybody uses the hash function on the same

1 person's name, they're going to get the same
2 output. Correct?
3 A Yes.
4 Q So the output has to be based on the
5 input?
6 A Yes.
7 Q Okay. You mentioned that hash functions
8 are not reversible. Are there any other
9 encryption techniques that are -- other than hash
10 functions that are not reversible?
11 A There is a class of functions called
12 one-way hash function -- I'm sorry, one-way
13 functions. And one-way functions, an example of a
14 one-way function is a hash function. I'm not
15 thinking as I sit here of other examples. But I
16 believe in the theoretical cryptography literature
17 there are other ways to achieve a one-way function
18 besides a hash function.
19 Q Then would it be safe to say that,
20 generally speaking, when a person says a one-way
21 function, they're typically talking about a hash
22 function?

1 A I think if you're not a professional
2 cryptographer, that's probably true.
3 Q What about the person of ordinary skill
4 in the art in this case?
5 A They would likely be referring to a hash
6 function.
7 Q Can you turn to Paragraph 5 of the '651
8 patent, specifically Lines 9 through 12.
9 A Do you mean column?
10 Q Yes, sorry, Column 5, Lines 9 through 12.
11 A All right. Okay.
12 Q And that section states, "The tokens 202
13 correspond to persons treated by healthcare
14 providers but do not reveal the identities of the
15 treated individuals."
16 Do you see that?
17 A Yes.
18 Q So essentially one token corresponds to
19 one person?
20 A Yes.
21 Q And if you could turn to your declaration
22 for the '651 patent, at Paragraph 56, please.

1 A Okay.
2 Q And the first full sentence in that
3 paragraph at the top of Page 21 states, "The third
4 party, for example, using an encryption server,
5 generates a request token for each individual in
6 the group based on the personally identifiable
7 information for each individual in the group."
8 Do you see that?
9 A Yes.
10 Q So that's referring to creating a token
11 based on the personally identifiable information
12 for each individual. Correct?
13 A Yes.
14 Q So that might be their name, date of
15 birth, and/or other information. Correct?
16 A I just have a citation here to the
17 patent, so I'm just going to review that.
18 I think that's correct.
19 Q So in that sense, the token is derived
20 from the personally identifiable information?
21 A Yes.
22 Q Just for clarity, going back to the

1 earlier discussion we had on public and private
2 keys for encryption.
3 Public-private keys where there is a key
4 that allows for decryption, that would be
5 considered by a person of ordinary skill in the
6 art a type of encryption method. Correct?
7 A Yes. For, you know, we're talking
8 outside of this patent.
9 Q And whether we're talking about
10 public-private key option or a hash function, if
11 one were to tokenize using one or the other of
12 those, they would take the personal information
13 from the individual and encrypt it either using
14 the public key or the hash function, depending on
15 the methodology that the person wants to use?
16 A I don't think the patent describes using
17 a public-private key system for that purpose. It
18 only describes using irreversible functions such
19 as a hash function.
20 Q Well, let me clarify my question. In
21 both using a public-private key system and a hash
22 function, both systems take the input and convert

1 it into an output that is, you know, not readable,
2 by a human at least. Correct?
3 A Both systems converted to an output
4 that's not readable by a human, but in one case
5 that output could be -- you can derive the input
6 again from the output, and in one case you can't.
7 Q Only if you have the key, though.
8 Correct?
9 A Or if there's some other security issue
10 that happens.
11 Q One -- I read in the papers within the
12 record of this case that hash functions typically
13 result in a set number of characters for the
14 output.
15 Is that typical operation for hash
16 function?
17 MR. STEPHENS: And are you referring to a
18 particular document, Justin?
19 MR. OLIVER: Not off the top of my head,
20 no. But we can talk just generally about hash
21 functions, if that would be helpful.
22 A So let me hear the question, then the

1 general question.
2 Q My understanding is that hash functions
3 typically have a set number of characters for an
4 output.
5 Is that a fair characterization?
6 A Yes.
7 Q So in that regard, there is a -- I mean,
8 a set number of possible hash functions for an
9 input. Correct?
10 A Yeah. The standard hash functions to
11 date tend to have 160 bits, but it can vary by
12 hash function.
13 Q Is it ever then the case that two
14 different inputs could theoretically result in the
15 same output?
16 A The whole concept of a hash function, the
17 definition in cryptography is that you can't find
18 two inputs that could hash to the same output.
19 Q And is that just because of the size of
20 the output?
21 A Yes. And the strength of the hash
22 function.

1 Q But if there are a limited number of
2 characters, then there are only a limited number
3 of possible outputs. Correct?
4 A Right. Two to the 160 outputs for
5 160-bit function, you know, these things start to
6 approach the number of particles in the universe.
7 And so you end up with the case that it's more
8 likely that the world would spontaneously erupt
9 than that you would find two inputs that hash to
10 the same output.
11 Q Okay. In a public-private key system,
12 what's the means for decryption of an encrypted
13 piece of information?
14 A You apply the reverse transform with the
15 private key and you get a decryption.
16 Q So the mechanism or the means is that you
17 need the private key to decode?
18 A Well, you would need to know what the
19 public key function was and what the decryption
20 function is, and you need to have the private key.
21 MR. OLIVER: I'm going to switch to
22 discussing Evenheim. But since we're getting

1 close to what would be an hour, maybe this is a
2 good time for a short break. Let's say ten
3 minutes?
4 THE WITNESS: Sure.
5 (A recess was taken.)
6 (Exhibit 1005, previously marked, not
7 attached.)
8 BY MR. OLIVER:
9 Q Dr. Rubin, can you turn to the Evenheim
10 reference, please.
11 A Okay, I'm there.
12 MR. OLIVER: Which has been marked, just
13 for the record, as Exhibit 1005.
14 Q And I just want to go over some basics
15 for which I think there is agreement, but I just
16 want to make sure.
17 If you could turn to Figure 4 of
18 Evenheim.
19 A Okay.
20 Q I think in our last deposition we talked
21 about this a little bit. But just so we're on the
22 same page, on the far left we have a section

1 called the Pharmaceutical Company. Correct?
2 A Yes.
3 Q And then in the middle position we have
4 what's referred to as Crossix?
5 A Yes.
6 Q And that's where the data aggregator is.
7 Correct?
8 A Yes.
9 Q And on the far right we have what are
10 referred to as health plans or PBMs. Correct?
11 A Yes.
12 Q And those are the data sources that have
13 the records to be searched. Correct?
14 A Yes.
15 Q All right. So just going through a few
16 things.
17 On the far left, within the User section,
18 there is, I'll call it a Step 2, for lack of a
19 better term. And it refers to the user interface
20 that uploads identifiable patient lists.
21 Do you see that?
22 A Yes.

1 Q So those patient lists are coming from
2 the user, and they're being sent or uploaded to
3 the aggregator. Correct?
4 A Yes.
5 Q And then within the Aggregator box there
6 are Steps 3 and 4. And Step 3 involves at least
7 encrypting patient lists and query. Correct?
8 A Yes.
9 Q And then in Step 4 that query is
10 distributed to all available data sources.
11 Correct?
12 A Yes.
13 Q So that means sending the query to the
14 data sources for the searching to take place.
15 Correct?
16 A Yes.
17 Q All right. Can you look at Paragraph 73
18 of your '651 declaration.
19 A Okay.
20 Q And at the first full sentence at the top
21 of Page 35 -- I'm sorry. Did I say 73?
22 A You did.

1 Q Okay. Apologies. At the first full
2 sentence at the top of Page 35, it states that the
3 aggregator processor receives queries from
4 consumer entity processors, and from the queries
5 generates search requests for the source entity
6 processors.
7 Do you see that?
8 A I see that.
9 Q And what does it mean for the aggregator
10 to generate search requests based on the
11 information from the user?
12 A Okay. Can you please repeat the
13 question?
14 Q Sure. What does it mean for the
15 aggregator to generate search requests based on
16 what comes from the user?
17 A Sorry, I'm just reading around for
18 context.
19 Q And if it helps you, what I'd like to
20 talk after this question is around Column 8, Lines
21 30 through 48, if that context helps.
22 A Lines 30 through?

1 Q Forty-eight.
2 A Where, simply stated?
3 Q Yes.
4 A So what he's saying is there's a formal
5 language that's used to create queries that will
6 help answer the specific questions that the
7 researcher is looking for.
8 Q So based on that Column 8, Lines 30
9 through 48, it seems to be describing that the
10 aggregator takes the identity specifics that come
11 from the user for the list of patients that the
12 user is interested in, and does some sort of
13 conversion to that information before sending it
14 to the data sources. Correct?
15 A Yes.
16 Q And around Lines 37, 38, there is a
17 reference to that conversion involving shared
18 variable definitions mutually accepted by the
19 aggregator and the source entities.
20 Do you see that?
21 A Yes.
22 Q And what's that referring to?

1 A In order for the communication to be
2 meaningful, the source entities and the aggregator
3 have to have some preagreed-upon language that
4 they can use to interact.
5 Q So in order to have the search be
6 successful, the aggregator has to use the language
7 that the database understands.
8 Is that fair?
9 A The data sources, yes.
10 Q Okay. Staying on Column 8 of Evenheim,
11 looking at Lines 13 through 18. Evenheim states
12 that what is important in the further application
13 of the instant method is that these
14 identity-disclosing specifics are part of a
15 large-enough list in the processing of a query so
16 that the query results will present sufficient
17 statistical distribution to protect the reverse
18 engineering of the result back to any individual
19 in the initial query list.
20 Do you see that?
21 A Yes.
22 Q And what does it mean that the list must

1 be large enough, in that context?
2 A It means that it will present a large
3 statistical distribution so that somebody can't
4 look at the results and figure out a particular
5 individual.
6 Q So that means you have to have enough
7 people in the list so that you're not going to be
8 able to identify any one of them from the results.
9 Is that fair?
10 A I think that's what it's saying.
11 Q And just on that point, if you could turn
12 to Column 13, Lines 62 to 67.
13 A Okay.
14 Q And there there's a reference to a
15 predetermined minimum number of individuals.
16 Do you see that?
17 A Yes.
18 Q So that's the same idea, that your list
19 that you're searching for has to have a minimum
20 number of people to be proper.
21 Is that fair?
22 A Let me just review this.

1 It talks about having a minimum number of
2 individuals included in a parameter list that is
3 sent.
4 Q And the parameter list is what's sent to
5 the -- ultimately sent to the data sources.
6 Correct?
7 A Well, it gets converted through the
8 common language that they have and then
9 communicated.
10 Q And you're referring to the conversion by
11 the aggregator?
12 A Yes.
13 Q All right. I'd like to contrast that
14 with something else that's discussed in Evenheim.
15 At Column 16, Lines -- well, full, if you could
16 read Column 16, Lines 5 through 32, please.
17 A Okay.
18 Q So just to start off with this, there is
19 reference that says, For each health plan, the
20 query engine runs a, what it calls a fuzzy
21 matching algorithm. Correct?
22 A Yes.

1 Q So we're talking about the query engine
2 on the data source side of the equation?
3 A Yes.
4 Q And then further down in that paragraph
5 there is reference around Line 18 to different
6 programs, a call center program and a website
7 program.
8 Do you see that?
9 A Yes.
10 Q And then that's referenced again in the
11 paragraph from Lines 22 through 32. Or at least
12 programs are.
13 Is that a fair characterization?
14 A I'm not sure what you're referring to.
15 Q Certainly. So starting around Line 27 or
16 maybe 26, it says, "The query engine determines
17 whether the number of participants in each program
18 and the percentage participants matched are above
19 a level that ensures consumer individual privacy
20 based on a statistical definition. If not, the
21 query engine responds with, Group name cannot be
22 analyzed because of privacy safeguards. Please

1 try to define a bigger group of users."
2 Do you see that?
3 A Yes.
4 Q So that seems to be saying that the query
5 engine at the data source looks to see the number
6 of people in this program being searched and the
7 percentage of people matched to make sure that
8 both are above a minimum level.
9 Is that correct?
10 A It doesn't say above a minimum level; it
11 says that they're above an appropriate level.
12 Q Okay. So they have to be above an
13 appropriate level. And if they are not above the
14 appropriate level, the data source says I can't
15 perform your search, essentially.
16 Is that fair?
17 A It won't -- yeah.
18 MR. STEPHENS: Objection. To form.
19 A It says it can't be analyzed.
20 Q Okay.
21 A Specifically it says, "Cannot be analyzed
22 because of privacy safeguards. Please try to

1 define a bigger group of users."
2 Q So essentially the data source is telling
3 the user when I search for hits I got too few and,
4 therefore, I can't give you the results. Why
5 don't you try again with a different request.
6 Is that a fair characterization?
7 A It's saying that it -- because of the
8 privacy safeguards, it can't analyze and it wants
9 a bigger group of users.
10 Q And the privacy safeguard that it's
11 referring there is that the size of the group and
12 the percentage of participants matched are not
13 appropriately high. Correct?
14 A Yes, based on a statistical definition.
15 Q And what would be an example of a
16 statistical definition?
17 A I'm not sure.
18 Q Well, what's generally the reason behind
19 using these appropriate levels in the context of
20 HIPAA?
21 A It has to do with protecting user
22 privacy.

1 Q Okay. Let's turn to the Murphy
2 reference, Exhibit 1009, please.
3 (Exhibit 1009, previously marked, not
4 attached.)
5 A Just a moment, because I didn't have that
6 one open.
7 Q No problem. Take your time.
8 A Okay, I've got it handy, so it's open
9 now.
10 Q All right. If you could turn to Page 553
11 of Murphy.
12 A Okay.
13 Q And if you look on the right hand towards
14 the bottom, there are paragraphs Numbered 1 and 2.
15 And the second one begins with, "An audit trail."
16 Do you see that?
17 A Yes.
18 Q And what's your understanding of an audit
19 trail in this context?
20 A It's a log that includes information
21 about the program that's running.
22 Q And in particular, the user ID, the time

1 of their query, number of patients returned are
2 the examples given in Paragraph 2. Correct?
3 A Yes.
4 Q And the program sort of continues to
5 analyze this, what it refers to as audit trail.
6 Correct?
7 A Yes.
8 Q And then in the next paragraph it states,
9 "In an abstract sense the key to the data
10 obfuscation method is to make attempts to discern
11 individuals in the database a recognizable pattern
12 by a computer algorithm."
13 Do you see that?
14 A Yes.
15 Q So the idea that Murphy is explaining
16 here is that it tracks the searches in some manner
17 that are performed by a user to see if the
18 algorithm can detect patterns that would indicate
19 some sort of attack.
20 Is that at a top level a fair
21 characterization?
22 A Yeah.

1 Q And what's the concern with a user
2 repeatedly putting in a number of the same query
3 or narrowing parameters of a query, what would a
4 POSA understand to be the risk of allowing the
5 user to do that?
6 A To be able to learn information that is
7 supposed to be private.
8 Q And in the context of HIPAA that would
9 be, for instance, a particular patient's identity,
10 for example?
11 A Right.
12 Q If you could take a look at Page 554. On
13 the left-hand side about two-thirds of the way
14 down there's a paragraph that begins, "As the
15 numbers."
16 Do you see that?
17 A Yes.
18 Q And if you want to read that paragraph,
19 there's a discussion of a history table. But why
20 don't you take a moment to read that.
21 A Okay.
22 Q So it seems that that history table

1 that's being referred to there is what's used to
2 perform that audit trail. It's the record of the
3 user queries.
4 Is that fair?
5 A It doesn't say that this is the audit
6 trail.
7 Q It does indicate that the history table
8 contains for each query the date, time, the user
9 ID, the number of patients returned, which matches
10 what's in the Paragraph 2 we talked about on Page
11 553. Correct?
12 A So in -- the Paragraph 2 gave a few
13 examples, and they're the same examples that are
14 given here.
15 Q If you could turn to Page 552 of Murphy.
16 A Okay.
17 Q And on the right-hand side about
18 two-thirds of the way down there's a paragraph
19 that begins, "A fairly general user base."
20 Do you see that?
21 A Yes.
22 Q If you could review that paragraph,

1 please.
2 A Okay.
3 Q And the last sentence there states that
4 "these two factors heighten concerns about patient
5 confidentiality using a general query tool, and it
6 became imperative that a single individual could
7 not be identified through the user interface."
8 Do you see that?
9 A Yes.
10 Q And why is it imperative that a single
11 individual could not be identified through a user
12 interface?
13 A To protect that person's privacy.
14 Q And what would a person of ordinary skill
15 in the art understand to be some of the manners of
16 attack through a user interface that would allow
17 for identification of a particular patient?
18 A I can't think of any examples. I didn't
19 cover that in my report.
20 Q Would queries that return only one or two
21 patient records be of a concern to a POSA?
22 A Yes.

1 Q And would that be because if the query
2 returns records for only one or two people, then
3 the user might be able to figure out who those
4 people are?
5 A That's a concern.
6 Q Do you have handy the petition for the
7 '375 patent? And if not, I can put it in the
8 chat.
9 A I probably have it, but I think it would
10 be faster if you put it in the chat.
11 Q Sure. Give me a moment, please.
12 A Just to have it, I am opening up my '375
13 declaration.
14 Q Let me know when you have that.
15 A Got it.
16 Q Great. All right. If you could turn to
17 Page 16 of the petition.
18 A Okay. PDF 24?
19 Q Correct.
20 A Okay.
21 Q And I'd like to talk about some of the
22 claim language of the '375 patent, but I want to

1 do it in the context of the naming convention in
2 the petition, and specifically Limitation 7.a
3 through 7.c. So if you want to take a quick look
4 at those, 7.a. And this is just the claim
5 language on the left column. So if you want to
6 take a look at those three paragraphs, or three
7 sections, rather, that would be great.
8 A Okay.
9 Q All right. I just want to make sure
10 we're on the same page here. So if we look at
11 Limitation 7.a of the '375 patent and the petition
12 at Page 16, it refers to a data server device.
13 Correct?
14 A Yes.
15 Q So that's the server that includes the
16 information to be searched. Correct?
17 A Yes.
18 Q And then if we look at 7.b, it
19 characterizes that data server device by saying
20 that it's for producing healthcare information
21 that characterizes a group of a number of
22 individuals. Correct?

1 A Yes.
2 Q And it goes on to make clear that those
3 individuals are identified in a request for the
4 healthcare information that characterizes the
5 group. Correct?
6 A Yes.
7 Q All right. So we have a request for the
8 healthcare information. And I want to talk about
9 that in the context of 7.c. if you can turn down
10 to there.
11 A Okay.
12 Q And 7.c states, "Wherein the request for
13 healthcare information." So it seems to be
14 talking about the request that was identified in
15 7.b. correct?
16 A That's my understanding of how patents
17 work.
18 Q All right. And it says that, "The
19 request for healthcare information is sent to an
20 encryption server that is configured to determine
21 if the number of individuals in the request is at
22 least a defined minimum number of individuals."

1 Correct?
2 A Yes.
3 Q All right. So that request for
4 healthcare information is the request that is sent
5 to the encryption server. Correct?
6 A Yes.
7 Q So that would typically be by a user or
8 some similar position's entity. Correct?
9 A Sure.
10 Q And then it seems that the -- going back
11 to 7.b. The data server device is for producing
12 healthcare information that characterizes a group
13 of a number of individuals in that request for
14 healthcare information. Correct?
15 A Yes.
16 Q So that presumes that that request
17 ultimately makes it to the data server?
18 A In some -- in one form or another.
19 Q And when you say "in one form or
20 another," that might be similar to what we
21 discussed before, that there might be some use of
22 common language between the encryption server and

1 the data server to make sure they're speaking the
2 same language.
3 Is that fair?
4 A What I was referring to is that if you
5 look at the '375 patent, it describes replacing
6 user-identifiable information with tokens.
7 Q Oh, understood. Okay. Thank you.
8 Can you turn back to the '651 patent.
9 A Okay.
10 Q And if you could go to Column 12.
11 A Okay.
12 Q Actually, we can stay in the '375
13 petition.
14 A Okay, I'm back.
15 Q I'm sorry. I'll make it simple. We'll
16 stick in the '651 patent, Column 12, Line 67.
17 A '651, Column 12, Line 67? So the last
18 line on the page in Claim 7?
19 Q Yeah. So the portion of Claim 7 that
20 states, "Receiving a request from a user device
21 for information that characterizes a group."
22 Do you see that?

1 A Yes.
2 Q What's your understanding of the scope of
3 information that characterizes a group?
4 A I just looked through my report, and I
5 don't see anywhere that I describe what that scope
6 is, so that would be a new opinion.
7 Q I'm sorry, what was the last thing you
8 said?
9 A So that would be a new opinion, if I were
10 to try to come up with that on the fly.
11 Q I'm just asking to sort of understand the
12 scope of Claim 7. You did review Claim 7.
13 Correct?
14 A Yes.
15 Q So do you have a sense of what
16 information that characterizes a group would be?
17 MR. STEPHENS: Objection. Beyond the
18 scope.
19 A I would just take the plain and ordinary
20 meaning. I haven't construed that any other way.
21 Q Let me give an example, and you can take
22 a look at Claim 7 and see what your thoughts are.

1 Could a request within the context of
2 Claim 7 be, Here are a list of 100 patients. I'd
3 like to know the number of patients within that
4 group that have heart disease?
5 MR. STEPHENS: Objection.
6 Justin, is there a portion of the
7 declaration that you're referring to?
8 MR. OLIVER: No. I'm just asking about
9 the scope of Claim 7.
10 MR. STEPHENS: I will maintain my
11 objection. Beyond the scope.
12 A I have not looked at that question yet.
13 Q Well, let me ask this then.
14 Is there anything -- and take your time
15 and read Claim 7. Is there anything in Claim 7
16 that would preclude the user request being, of
17 these 100 people, please let me know the number
18 that have heart disease?
19 MR. STEPHENS: Objection. Beyond the
20 scope. This is a cross on the testimony that was
21 offered in the declaration.
22 A I can't say. I haven't looked at that.

1 Q Well, if you read Claim 7 now, is there
2 anything that you can see in Claim 7 that would
3 preclude that?
4 A I don't want to give on-the-fly opinions,
5 so I'll -- I will say that I don't know.
6 Q So you have no basis to say that that
7 would be excluded from the scope of Claim 7?
8 MR. STEPHENS: Mischaracterizes the
9 witness's testimony.
10 A I can't say one way or the other.
11 Q Is there anything that you're aware of
12 within the scope of Claim 7 -- and again, take
13 your time to read the claim -- that states limits
14 on what the user's request has to be?
15 MR. STEPHENS: Objection. Beyond the
16 scope.
17 A I have not looked at whether there is
18 anything other than the language in the claim that
19 has some limitations on it, but I haven't
20 considered that question.
21 Q Yeah, and I'm just asking, if you could
22 read Claim 7 now, if you could see anything that

1 would preclude that option?
2 A I'm not prepared to answer questions that
3 are not from my declaration.
4 Q Are you aware of anything in the '651
5 patent that limits the nature of the query to the
6 database?
7 MR. STEPHENS: Objection. Form. And
8 beyond the scope.
9 A I haven't considered that question before
10 and it's not in my report, so I don't know.
11 Q If you could look in the -- your '651
12 declaration.
13 A Okay.
14 Q At Paragraph 56.
15 A Okay.
16 Q And there you refer to requests for
17 deidentified data that characterizes a group of
18 identified individuals.
19 Do you see that?
20 A Yes.
21 Q And that deidentified data may contain
22 information regarding patients' pre or post

1 operation encounters with healthcare facilities.
2 Is that correct?
3 A Yes.
4 Q So would it be fair that your reference
5 here to "characterizes a group" could be the
6 number of people that have had a particular
7 operation?
8 A Yes.
9 Q So the request might be, for these 50
10 people, how many people have had knee surgery?
11 A I don't give that example, but I don't
12 see the problem with that.
13 MR. OLIVER: All right. I might not have
14 much more, so give me -- let's go off the record
15 for ten minutes.
16 (A recess was taken.)
17 BY MR. OLIVER:
18 Q Dr. Rubin, I have a few more questions.
19 Going back to something we discussed earlier with
20 respect to public-private key systems.
21 With the typical public-private key
22 system, is it fair to say that one would expect

1 that if the same name is encrypted with a public
2 key at two different times, that the output would
3 be the same?
4 A Not with the standard systems used today.
5 They all use randomized encryption.
6 Q Well, are there systems of public-private
7 keys where the input is going to be the same --
8 the output is going to be the same for the input
9 when used at different times?
10 A Not in any of the currently used systems.
11 That is something you could program a computer to
12 do, but it would be deprecated. All the standards
13 today and all of the systems that I know of in use
14 use randomized encryption.
15 Q How does the private key then decrypt the
16 information?
17 A So by randomized encryption, typically
18 that's done by pre-pending some random value to
19 the input. And then after you decrypt, you just
20 ignore that part of the message.
21 Q So a portion of the -- well, let me
22 rephrase that.

1 So the encryption of the same name twice
2 can be linked together by the person who has the
3 key?
4 A If I'm understanding your question, we're
5 talking generally in the world outside of this
6 case. If someone has the private key and somebody
7 else encrypts a name, two different people encrypt
8 a name, the person that has both private keys -- I
9 assume there might be different keys -- would be
10 able to link that because they would be decrypting
11 the same thing once they threw away the random
12 factor.
13 Q Can you turn to Exhibit 2006, which is
14 the HIPAA privacy rules that we looked at earlier.
15 A Yes.
16 Q Looking at Section 164.514(b), there is
17 what I think we've been calling the expert
18 determination method for deidentification.
19 Is that fair?
20 A I don't recall us discussing it, but
21 that -- I am familiar with that.
22 Q Yeah. Sorry. I didn't mean today. I

1 just meant in general in this case.
2 A Okay.
3 Q Under (b)(1), or in (b)(1), there is a
4 reference to "a person with appropriate knowledge
5 of and experience with generally accepted
6 statistical and scientific principles and methods
7 for rendering information not individually
8 identifiable."
9 Do you see that?
10 A Yes.
11 Q What would the person of ordinary skill
12 have understood, you know, at the time HIPAA came
13 out and prior to the patents that we've been
14 talking about today, the '651 patent for instance,
15 what would the person of ordinary skill understand
16 to be generally accepted statistical principles
17 and methods for deidentification?
18 A I don't know. I haven't formulated an
19 opinion on that.
20 Q And what about scientific principles and
21 methods; what would be some examples of scientific
22 principles and methods that a person of ordinary

1 skill would have been aware of at the time?
2 A Same answer. I haven't formulated an
3 opinion on that.
4 Q Do you know what would have been known at
5 that time with respect to either statistical or
6 scientific principles that were available to a
7 person of ordinary skill in the art?
8 A I do. But I would -- to answer a
9 question under oath, I would have to give that
10 some thought and provide an opinion, which I am
11 not prepared to do in this case because it's not
12 in my report.
13 Q Well, if you do know some examples, could
14 you at least share what some of those examples
15 would be, please?
16 A I didn't say that I have examples that
17 are handy. I just said that I know what this is.
18 I just -- it's not something I have worked on, and
19 I'm not -- I know I'm not supposed to perform
20 on-the-fly analysis.
21 Q Well, you're supposed to answer the
22 questions that are posed. So I'm asking if you

1 know of accepted scientific principles that were
2 known at the time for deidentification?
3 A If you ask me a particular principle, I
4 can think about whether or not it would have been
5 an accepted one, but I don't have a list, and I
6 haven't prepared to do that.
7 Q So sitting here today, you are not sure
8 what specific scientific principles were known at
9 the time that these rules were released?
10 A That's not what I said.
11 MR. STEPHENS: Objection. Beyond the
12 scope.
13 A That's not what I said.
14 Q Well, if you do know, can you tell me
15 what some examples would be?
16 A I think that coming up with examples is
17 something that would require me to do some work.
18 I'm here to answer questions about my report, not
19 to do new analysis.
20 Q Okay.
21 A So while this is something that I do
22 know, I don't have examples that I've prepared.

1 Q Well, I'm just trying to understand the
2 question so the record is clear.
3 You're saying you do have examples, but
4 you can't provide them right now, so --
5 A No. That's not what I said.
6 Q So you don't know of examples?
7 A I am saying that I have not prepared any
8 examples. That is something that would require
9 some work.
10 Q And I'm just asking whether, sitting here
11 today, you know of any examples?
12 MR. STEPHENS: And, Counsel, could I ask,
13 are you asking about a specific portion of his
14 report you can direct us to?
15 MR. OLIVER: I'm sorry. You're allowed
16 to do one-word objections. No speaking objections
17 are permitted. So please, if you have an
18 objection, make it with one word and that's it. I
19 am asking my questions.
20 MR. STEPHENS: Objection. Beyond the
21 scope.
22 Q Dr. Rubin, sitting here today, are you

1 aware of examples of what would be considered
2 generally accepted scientific principles and
3 methods that a person of ordinary skill in the art
4 would have known, you know, a day prior to the
5 '651 patent or at the time that HIPAA was
6 released?
7 A Methods for what?
8 MR. STEPHENS: Objection. Beyond the
9 scope.
10 Q Methods for deidentification under HIPAA
11 Rule b)(1) that we're discussing.
12 A I would have to look that up and do some
13 research. It's not something I know off the top
14 of my head. But it's something that is within my
15 area of expertise.
16 Q So I think we're getting to clarity. You
17 can't give any examples here today because off the
18 top of your head you're not aware of any, sitting
19 here today?
20 A This is the kind of thing that I prepare,
21 like the things that are in my report were well
22 thought out and researched. And off the top of my

1 head, sitting here, I don't have examples of
2 things that are not in my report.
3 Q And so that, sitting here today, you're
4 not aware of any examples that would qualify?
5 A Same answer I just gave.
6 Q Which is you -- you're not aware of any
7 examples, sitting here?
8 A I mean, there is a record. You can see
9 what my answer was or I can repeat it.
10 Q Well, I'd like to just be clear whether
11 you are not willing to provide examples or you're
12 not -- or you just don't know examples?
13 A The answer is that I have a lot of things
14 in my report. I submitted several reports in this
15 case. Examples of this is not something that I
16 prepared. And so I don't want to give on-the-fly
17 analysis, on-the-fly opinions to generate examples
18 that I haven't thought about before and later
19 might consider that weren't good examples.
20 So I'm not prepared to answer that.
21 Q So that's what I'm trying to get to. You
22 don't want to answer, or you don't know of

1 examples? Like, I just want to know whether you,
2 right now, sitting here today, know of examples
3 that would qualify under this HIPAA rule as
4 generally accepted scientific principles.
5 If you don't know, you can tell me you
6 don't know.
7 A I understand what you're asking.
8 MR. STEPHENS: Objection. Beyond the
9 scope.
10 A I think the best answer I can give you is
11 that I don't feel comfortable giving answers that
12 are not researched and well thought out. And so
13 if you're asking for things that are not in my
14 report, then I'm not willing to answer because I,
15 you know, am not sure I would give a correct or
16 complete answer.
17 Q So what you just said there is you're not
18 willing. And if, you know, if you're going to
19 leave it that you're not willing, that's fine.
20 But I'm just trying to make clear for the record
21 so the judges know whether you know of examples or
22 you're just not willing to give them?

1 A No, I am not willing to --
2 Q If you can provide any clarity on that,
3 please do so.
4 A Okay. What I am not willing to do is to
5 make up new theories. I am willing to answer your
6 question. And I'm trying to answer your question.
7 But I don't want to provide opinions that are new.
8 And so I don't have any examples that I've thought
9 out and that I'm prepared to offer for this
10 question.
11 Q And just to be clear, I'm not asking
12 whether you're comfortable giving them. I'm
13 asking of whether you know, sitting here today,
14 what those examples might be?
15 A I don't have any examples that I
16 researched and are well thought out and that are
17 in my report, and so I don't have anything that I
18 could give you.
19 Q All right. Then we will leave it at
20 that.
21 MR. OLIVER: I have no further questions.
22 MR. STEPHENS: All right. I think we

1 will do redirect, but I would like a little time
2 to prepare for that. Let's take 20 minutes, if
3 that's all right for the folks on this call.
4 MR. OLIVER: That's fine.
5 MR. STEPHENS: Actually, why don't we
6 return at 11:50 eastern.
7 Is that okay with you, Counselor?
8 MR. OLIVER: Yes.
9 (A recess was taken.)
10 EXAMINATION BY COUNSEL FOR PATENT OWNER
11 BY MR. STEPHENS:
12 Q Welcome back, Dr. Rubin.
13 A Thank you.
14 Q Do you recall being asked by petitioner's
15 counsel about claim constructions that have been
16 applied in this proceeding?
17 A Yes.
18 Q And there is a table of constructions
19 that were provided in the petition and reproduced
20 in Paragraph 70 of your '651 declaration.
21 Do you recall that?
22 A Yes.

1 Q Have you independently derived the
2 constructions in this table?
3 A No.
4 Q Where did they come from?
5 A These were used by the petitioner.
6 Q They were set forth in the petition?
7 A Yes.
8 Q Did you render an opinion as to whether
9 these constructions are correct?
10 A No.
11 Q Why not?
12 A That wasn't my assignment. My assignment
13 was to perform, you know, an analysis of prior art
14 references and if they invalidate. And so I used
15 petitioner's constructions in my analysis.
16 Q Have you applied the constructions in
17 this table in rendering your opinions?
18 A I did.
19 Q And your opinions ultimately were that
20 the prior art raised in the petitions did not
21 render obvious the challenged claims?
22 MR. OLIVER: Objection. Leading.

1 A That's correct.
2 Q I'll rephrase.
3 What was your ultimate determination as
4 to the ground in these petitions?
5 A That the prior art references did not
6 render the patents invalid.
7 Q You recall being asked by petitioner's
8 counsel about the construction of token?
9 A Yes.
10 Q What is the construction of token that
11 petitioner provided in its petition?
12 A An identifier associated with an
13 individual that does not reveal the identity of
14 the individual.
15 Q And do you recall a discussion with
16 petitioner's counsel about reversible encryption
17 and hash functions?
18 A Yes.
19 Q Based on your review of the patents at
20 issue, were reversibly-encrypted PII constituted
21 token within the meaning of these patents?
22 A No.

1 MR. OLIVER: Objection. Leading.
2 A No.
3 Q Why not?
4 A Because these patents are written through
5 the lens of HIPAA. And in HIPAA if you have
6 reversible encryption for encryption of
7 personally -- of PHI, then you are not in
8 compliance. And so within these patents,
9 reversible token would not -- reversible
10 information that was encrypted that way would not
11 constitute a token.
12 Q And so you're -- based on the testimony
13 you just gave, are you interpreting the claims
14 through the lens of HIPAA?
15 A Yes, I am.
16 Q What role, if any, does HIPAA have to
17 play with regard to the inventions in the '651,
18 '375, '012 and '685 patents?
19 A So HIPAA is the framework for these
20 inventions. It assumes that the operations take
21 place in a HIPAA-compliant fashion.
22 Q What leads you to that opinion?

1 A So if we -- let me turn to the '651
2 patent. And this is -- let's get to the right
3 column. So if you look at the Background of the
4 Invention, the Column 1, Line 25, it says, "The
5 present disclosure relates to processing and
6 transmitting personal data, the dissemination of
7 which is restricted by federal law."
8 And then throughout the patent
9 specification it talks about HIPAA, and there's no
10 disclosure in here that would not relate to HIPAA.
11 Q Is there anything in the claims that
12 supports your opinion?
13 A So, yes. If we look at Claim 1, the
14 producing element, the second producing element,
15 it talks about an identity of the individual being
16 unattainable from the produced information. And
17 the next element it talks about characteristics of
18 the group of individuals absent authorization from
19 the individuals. These are concepts that come
20 from HIPAA.
21 Q Now, in Paragraph 60 of your '651
22 declaration, can you turn there for a moment.

1 A Okay. I'm there.
2 Q The fourth line down, there's a sentence
3 that begins, "While the inventive technology is
4 not limited to systems and methods that operate
5 within the constraints of HIPAA, HIPAA nonetheless
6 features prominently in examples described in the
7 specification of the '651 patent, the prior art
8 applied in the petition, and the obviousness
9 analyses of the petitioner and its witness,
10 Dr. Clark."
11 Do you see that?
12 A Yes.
13 Q Could you explain what you meant by "the
14 inventive technology is not limited to systems or
15 methods that operate within the constraints of
16 HIPAA"?
17 A Yes. So I was referring here to the fact
18 that HIPAA only applies in the United States. But
19 if this is referring to something outside the
20 United States, there would be some federal
21 framework, as I pointed to in the Background of
22 the Invention. But within the United States it

1 would be HIPAA that would apply.
2 Q Are you aware of any context in the
3 United States in which HIPAA would not apply to
4 the claims in these patents?
5 A No.
6 Q And do you recall being asked by
7 petitioner's counsel about the concept of
8 tokenization?
9 A Yes.
10 Q And petitioner's counsel referenced
11 Paragraph 54 of your '651 declaration.
12 Do you recall that?
13 A Yes.
14 Q And specifically he referenced the last
15 sentence in Paragraph 54, which states, "Although
16 tokenized health data" has been viewed -- or "had
17 been used for other purposes prior to the '651
18 patent, it had not been used in a particular
19 context or manner described in the '651 patent."
20 Do you recall that?
21 A Yes.
22 Q I'd like to ask just a few questions in

1 that regard.
2 Based on your review of the prior art in
3 these proceedings, did any of those prior art
4 references use tokens in the manner claimed in the
5 patents at issue?
6 A No.
7 MR. OLIVER: Objection. Leading.
8 Q I'm sorry, can you repeat your response,
9 Doctor --
10 A I said no.
11 Q Are you aware of any other art that
12 applies tokenization in the same manner claimed in
13 the patents?
14 A No.
15 Q Are the inventions claimed in these
16 patents directed to mere tokenization techniques?
17 A No. They have to do with a specific way
18 of using tokenization.
19 Q Do you have a copy of Exhibit 2006
20 available?
21 A Yes.
22 Okay. I'm there.

1 Q And petitioner's counsel asked you a
2 number of questions about the provisions of the
3 HIPAA privacy rule set forth in Exhibit 2006.
4 Correct?
5 A Yes.
6 Q And you recall questions related to
7 Subsection C of the privacy rule?
8 A Yes.
9 Q Could you please take a moment to read
10 Subsection C.
11 A Okay.
12 Q What does this provision pertain to?
13 A This has to do with reidentification. It
14 has to do with a covered entity assigning a code
15 that allows deidentification, and then it has two
16 provisions for that.
17 Q And what are those two provisions?
18 A That the code is not derived from the
19 related information about the individual and is
20 not capable of being translated to the identity or
21 the individual. And that's -- that's Derivation
22 1. And also the security one, which says that the

1 covered entity does not use or disclose the code
2 or other means of record identification for any
3 other purpose, and does not disclose the mechanism
4 for reidentification.
5 Q So the derivation provision is set forth
6 in Subection (c)(2)?
7 A Yes.
8 Q And then there exists a security
9 provision in Subsection (c)(2)?
10 A Yes.
11 Q Which of these provisions are required to
12 use a valid reidentification code under HIPAA?
13 A They're both required.
14 Q So even if the security requirement were
15 not -- even if the reidentification code did not
16 comply with the security requirement -- strike
17 that.
18 Even if the reidentification code did not
19 comply with the derivation requirement, by itself
20 that would not comply with HIPAA?
21 A That's correct.
22 MR. OLIVER: Objection to form. Leading.

1 A That's correct.
2 Q Would the reversibly-encrypted
3 reidentification code that was derived from PII
4 satisfy the provisions under Subsection (c)?
5 MR. OLIVER: Objection. Leading.
6 A No.
7 Q Now, does Subsection (c) apply only to
8 decryption keys?
9 MR. OLIVER: Objection. Leading.
10 A No.
11 Q And you offer an opinion -- strike that.
12 What else could Subsection (c) apply to?
13 A Any means of reidentification that
14 doesn't satisfy the derivation in the security
15 requirements.
16 Q And did you offer an opinion that that
17 would include Landi's encrypted ID?
18 A Yes.
19 MR. OLIVER: Objection. Scope.
20 Q Do the provisions in Subsection (c) apply
21 to tokens that do not allow for reidentification?
22 MR. OLIVER: Objection. Leading.

1 A No.
2 Q Do the tokens described in the patents at
3 issue here violate HIPAA?
4 MR. OLIVER: Objection. Leading.
5 A No.
6 Q Why not?
7 A Because they satisfy the requirements of
8 the HIPAA rules. There is the deidentification is
9 not reversible.
10 MR. STEPHENS: Thank you, Dr. Rubin.
11 No further questions.
12 MR. OLIVER: I have some redirect, but I
13 could use just three minutes off the record before
14 I do.
15 (A recess was taken.)
16 EXAMINATION BY COUNSEL FOR PETITIONER
17 BY MR. OLIVER:
18 Q Dr. Rubin, in your declarations did you
19 provide any specific claim constructions of your
20 own?
21 A I don't recall providing any, but if
22 they're in my declaration then my declarations

1 speak for themselves.
2 Q You're not offering here today any
3 constructions that were not provided in your
4 declaration, are you?
5 A Right.
6 Q You discussed the '651 patent at Column
7 1, Lines 25 through 27. Can you turn there.
8 A Yes.
9 Q And that discusses that the present
10 disclosure relates to processing and transmitting
11 personal data, the dissemination of which is
12 restricted by federal law.
13 Do you see that?
14 A Yes.
15 Q And if I'm understanding you correctly,
16 you're interpreting that to mean at least HIPAA?
17 A Right, within the U.S. it would be HIPAA.
18 Q Are there other federal laws directed to
19 the dissemination of personal information or
20 personal data?
21 A I don't know, sitting here. There
22 probably are, but HIPAA is the one that I think is

1 most familiar to most people.
2 Q And am I understanding you correct that
3 your position is because of a statement such as
4 this one in the '651 patent, that a person would
5 interpret what's described as being
6 HIPAA-compliant?
7 Is that fair?
8 A There are statements throughout the
9 patent, for example, Column 4, Line 40, where it
10 talks about HIPAA. And the rest of the patent
11 specification is consistent with HIPAA, and the
12 claims are consistent with HIPAA. So the
13 combination of all of these statements is what
14 leads me to that.
15 Q So if I'm understanding you correctly, if
16 a document says that it's intended to comply with
17 HIPAA, you would expect that a person of ordinary
18 skill would implement it in a manner that is
19 HIPAA-compliant?
20 A Well, if a patent is designed for HIPAA,
21 as this one clearly is, then I assume that if one
22 of ordinary skill in the art were to practice that

1 patent, they would do it in a way that was
2 compliant with HIPAA.
3 Q And HIPAA rules existed prior to the
4 patents we're talking about here today, including
5 the '651 patent. Correct?
6 A Yes.
7 Q And the HIPAA rules that are relevant for
8 our discussion are primarily the ones -- well, let
9 me rephrase that. The HIPAA rules that we have
10 been discussing here today are those shown in
11 Exhibit 2006. Correct?
12 A Those were the ones we discussed, yes.
13 Q So your characterizations of what's
14 required by the rules shown in Exhibit 2006 would
15 have been understood by a person of ordinary skill
16 in the art, reading those rules at the time?
17 A Could you say that again, please?
18 Q Sure. Your interpretation of the HIPAA
19 rules set forth in 2006 are from the point of view
20 of a person of ordinary skill in the art.
21 Correct?
22 A Yes.

1 Q And the person of ordinary skill in the
2 art would have known that or would have known the
3 interpretations that you're setting forth when
4 these HIPAA rules were released. Correct?
5 A Upon reading the HIPAA rules, yes.
6 Q Dr. Rubin, between my ending my
7 cross-examination and Mr. Stephens' redirect, did
8 you discuss the substance of your testimony with
9 Mr. Stephens?
10 A Yes.
11 Q And what did you discuss with
12 Mr. Stephens?
13 MR. STEPHENS: Objection. Privileged.
14 I'll instruct the witness not to answer
15 the question to the extent it involves discussing
16 the content of any discussions.
17 MR. OLIVER: So just for clarity, are you
18 instructing the witness not to discuss any of the
19 discussions you had with Dr. Rubin between the end
20 of my cross-examination and the start of your
21 redirect?
22 MR. STEPHENS: That's correct.

1 MR. OLIVER: In that case, I have no
2 further questions.
3 MR. STEPHENS: Dr. Rubin, I've just got a
4 few questions.
5 MR. OLIVER: Can we just take a short
6 two-minute break before we do that?
7 MR. STEPHENS: Sure.
8 MR. OLIVER: Thank you.
9 (A recess was taken.)
10 MR. OLIVER: Counsel, before you begin,
11 my understanding from Rule 42.53 is that it allows
12 for seven hours of the initial examination, four
13 hours for the response, and then two hours for
14 what follows. And I believe we've done three, so
15 I'm not sure what your basis is for doing another
16 round of questions.
17 MR. STEPHENS: I would be happy to get
18 back to you on that if we go back off the record.
19 MR. OLIVER: Okay.
20 (A recess was taken.)
21 STEPHENS: Let's go back on the record,
22 please.

1 And patent owner has no further questions
2 for the witness.
3 (Off the record at 12:43 p.m. EST.)
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

1 ACKNOWLEDGMENT OF DEPONENT
2 I, AVIEL D. RUBIN, Ph.D., do hereby
3 acknowledge that I have read and examined the
4 foregoing testimony, and the same is a true,
5 correct and complete transcription of the
6 testimony given by me, and any corrections appear
7 on the attached Errata sheet signed by me.
8
9 _____
10 (DATE) (SIGNATURE)
11
12
13
14
15
16
17
18
19
20
21
22

1 C E R T I F I C A T E
2 I, Debra Ann Whitehead, E-Notary Public in and for
3 the Commonwealth of Virginia, do hereby certify:
4
5 That AVIEL D. RUBIN, Ph.D., the witness
6 whose deposition is hereinbefore set forth, was duly
7 sworn by me before the commencement of such
8 deposition and that such deposition was taken
9 virtually and is a true record of the testimony
10 given by such witness.
11
12 I further certify that the adverse party,
13 VIGILYTICS LLC, was represented by counsel at the
14 deposition.
15
16 I further certify that the deposition of
17 AVIEL D. RUBIN, Ph.D., occurred virtually, on
18 Monday, February 17, 2025, from 9:30 a.m. to 12:43
19 p.m. EST.
20
21
22

I further certify that I am not related to any of the parties to this action by blood or marriage, I am not employed by or an attorney to any of the parties to this action, and that I am in no way interested, financially or otherwise, in the outcome of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand this 20th day of February, 2025.

My commission expires: October 31, 2027

E-NOTARY PUBLIC IN AND FOR THE
COMMONWEALTH OF VIRGINIA

A
ability 5:14, 14:4, 14:6, 16:4
able 14:1, 23:7, 29:5, 43:8, 50:6, 53:3, 64:10
about 5:18, 7:9, 15:17, 15:19, 15:21, 16:14, 16:16, 18:14, 18:18, 20:10, 20:11, 22:21, 25:3, 26:10, 27:1, 27:6, 27:10, 28:7, 28:22, 29:10, 29:12, 30:21, 31:3, 33:9, 34:20, 37:21, 44:1, 45:1, 48:21, 50:13, 51:10, 51:17, 52:4, 53:21, 55:8, 55:14, 59:8, 65:14, 65:20, 67:4, 67:18, 68:13, 70:18, 73:15, 75:8, 75:16, 77:9, 77:15, 77:17, 79:7, 81:2, 81:19, 86:10, 87:4
above 45:18, 46:8, 46:10, 46:11, 46:12, 46:13
absent 6:4, 7:2, 77:18
abstract 49:9
accepted 41:18, 65:5, 65:16, 67:1, 67:5, 69:2, 71:4
access 8:3
achieve 30:17
acknowledge 91:3
acknowledgment 91:1
acronym 6:21
action 93:2, 93:4
actually 14:3, 25:13, 26:12, 57:12, 73:5
add 15:12
address 11:2
administrative 5:9
adversary 25:7
adverse 92:12
affect 5:14
after 11:6, 11:13, 40:20, 63:19
again 19:15, 34:6, 45:10, 47:5, 60:12, 87:17
aggregator 38:6, 39:3, 39:5, 40:3, 40:9, 40:15, 41:10, 41:19, 42:2, 42:6, 44:11
agree 24:18, 25:22, 29:19
agreement 37:15
algorithm 44:21, 49:12, 49:18
all 5:20, 6:1, 6:22, 8:3, 9:21, 27:22, 29:7, 29:18, 31:11, 38:15, 39:10, 39:17, 44:13, 48:10, 53:16, 54:9, 55:7, 55:18, 56:3, 62:13, 63:5, 63:12, 63:13, 72:19, 72:22, 73:3, 86:13
allow 13:9, 19:2, 20:5, 20:17, 23:19, 23:20, 27:18, 52:16, 83:21
allowed 68:15
allowing 28:17, 50:4
allows 33:4, 81:15, 89:11
already 7:19, 17:17
also 8:5, 14:2, 16:18, 20:13, 21:16, 81:22
alternative 12:11
although 9:10, 79:15
always 6:9
analyses 78:9
analysis 12:6, 66:20, 67:19, 70:17, 74:13, 74:15
analyze 47:8, 49:5
analyzed 45:22, 46:19, 46:21
ann 2:5, 92:2
anonymizing 10:3
another 13:7, 24:14, 56:18, 56:20, 89:15
answer 5:21, 6:5, 13:2, 25:4, 27:13, 41:6, 61:2, 66:2, 66:8, 66:21, 67:18, 70:5, 70:9, 70:13, 70:20, 70:22, 71:10, 71:14, 71:16, 72:5, 72:6, 88:14
answering 7:3
answers 71:11
any 5:10, 5:13, 5:21, 6:9, 7:12, 8:12, 12:11, 13:13, 16:22, 17:6, 17:9, 17:17, 30:8, 42:18, 43:8, 52:18, 58:20, 63:10, 68:7, 68:11, 69:17, 69:18, 70:4, 70:6, 72:2, 72:8, 72:15, 76:16, 79:2, 80:3, 80:11, 82:2, 83:13, 84:19, 84:21, 85:2, 88:16,

88:18, 91:6, 93:2, 93:3
anybody 29:22
anyone 7:15, 13:15, 24:18
anyplace 14:7
anything 8:10, 26:5, 28:6, 59:14, 59:15, 60:2, 60:11, 60:18, 60:22, 61:4, 72:17, 77:11
anywhere 17:13, 17:22, 18:15, 58:5
apologies 40:1
appeal 1:3
appear 91:6
application 42:12
applied 73:16, 74:16, 78:8
applies 28:10, 78:18, 80:12
apply 28:2, 36:14, 79:1, 79:3, 83:7, 83:12, 83:20
approach 36:6
appropriate 46:11, 46:13, 46:14, 47:19, 65:4
appropriately 47:13
area 69:15
around 16:19, 40:17, 40:20, 41:16, 45:5, 45:15
art 6:16, 6:20, 7:7, 31:4, 33:6, 52:15, 66:7, 69:3, 74:13, 74:20, 75:5, 78:7, 80:2, 80:3, 80:11, 86:22, 87:16, 87:20, 88:2
asked 6:11, 73:14, 75:7, 79:6, 81:1
asking 6:14, 10:15, 12:21, 19:3, 26:2, 58:11, 59:8, 60:21, 66:22, 68:10, 68:13, 68:19, 71:7, 71:13, 72:11, 72:13
assertion 6:4
assign 20:4, 27:17
assigning 81:14
assignment 74:12
associated 75:12
assume 24:12, 64:9, 86:21
assumes 28:17, 76:20
assuming 25:1
attached 4:10, 8:21, 19:20, 37:7, 48:4, 91:7
attack 49:19, 52:16
attempts 49:10
attorney 6:3, 93:3
audit 48:15, 48:18, 49:5, 51:2, 51:5
authorization 77:18
available 39:10, 66:6, 80:20
avenue 3:5
aviel 1:15, 2:1, 4:2, 5:2, 91:2, 92:5, 92:17
aware 14:7, 17:16, 17:21, 60:11, 61:4, 66:1, 69:1, 69:18, 70:4, 70:6, 79:2, 80:11
away 64:11

B

b 64:16
b)(1 65:3, 69:11
back 17:5, 26:7, 27:13, 28:3, 32:22, 42:18, 56:10, 57:8, 57:14, 62:19, 73:12, 89:18, 89:21
background 77:3, 78:21
base 51:19
based 30:4, 32:6, 32:11, 40:10, 40:15, 41:8, 45:20, 47:14, 75:19, 76:12, 80:2
basically 29:13
basics 37:14
basis 60:6, 89:15
became 52:6
because 17:12, 23:16, 25:1, 29:4, 29:7, 29:20, 35:19, 45:22, 46:22, 47:7, 48:5, 53:1, 64:10, 66:11, 69:17, 71:14, 76:4, 84:7, 86:3
been 5:3, 9:11, 9:12, 9:18, 12:1, 16:20, 37:12, 64:17, 65:13, 66:1, 66:4, 67:4, 73:15, 79:16, 79:17, 79:18, 87:10, 87:15
before 1:3, 2:5, 5:17, 5:19, 5:21, 7:22, 9:18, 10:8, 41:13, 56:21, 61:9, 70:18, 84:13, 89:6, 89:10, 92:7
begin 89:10
begins 48:15, 50:14, 51:19, 78:3
behalf 3:2, 3:9

behind
23:19, 47:18
being
14:1, 14:13, 14:18, 16:8, 17:20, 39:2, 46:6, 51:1, 59:16, 73:14, 75:7, 77:15, 79:6, 81:20, 86:5
believe
6:16, 30:16, 89:14
besides
30:18
best
71:10
best-positioned
26:3
better
26:5, 38:19
between
56:22, 88:6, 88:19
beyond
58:17, 59:11, 59:19, 60:15, 61:8, 67:11, 68:20, 69:8, 71:8
bigger
46:1, 47:1, 47:9
birth
32:15
bit
36:5, 37:21
bits
35:11
blood
93:2
board
1:3
both
13:2, 13:22, 33:21, 33:22, 34:3, 46:8, 64:8, 82:13
bottom
48:14
box
39:5
break
5:18, 5:19, 5:22, 24:19, 37:2, 89:6
brings
28:3
broken
23:18
business
25:12

C

c
83:4, 83:7, 83:12, 83:20
c)(2
82:6, 82:9
call
38:18, 45:6, 73:3
called
5:20, 30:11, 38:1
calling
64:17
calls
44:20
came
65:12
can't
28:9, 28:21, 34:6, 35:17, 43:3, 46:14, 46:19, 47:4, 47:8, 52:18, 59:22, 60:10, 68:4, 69:17
cannot
5:10, 45:21, 46:21
capability
23:2, 26:1
capable
81:20
case
8:16, 13:1, 13:12, 13:21, 14:3, 14:5, 14:19, 16:2, 18:4, 31:4, 34:4, 34:6, 34:12, 35:13, 36:7, 64:6, 65:1, 66:11, 70:15, 89:1
cases
25:8
center
45:6
certain
7:20, 19:9
certainly
45:15
certify
92:3, 92:12, 92:16, 93:1
challenged
74:21
characteristics
77:17
characterization
35:5, 45:13, 47:6, 49:21
characterizations
87:13
characterizes
54:19, 54:21, 55:4, 56:12, 57:21, 58:3, 58:16, 61:17, 62:5
characters
34:13, 35:3, 36:2
chart
12:14
chat
19:15, 19:18, 53:8, 53:10
citation
32:16
claim
12:14, 53:22, 54:4, 57:18, 57:19, 58:12, 58:22, 59:2, 59:9, 59:15, 60:1, 60:2, 60:7, 60:12, 60:13, 60:18, 60:22, 73:15, 77:13, 84:19
claimed
80:4, 80:12, 80:15
claims
74:21, 76:13, 77:11, 79:4, 86:12
clarify
33:20
clarity
12:10, 29:9, 32:22, 69:16, 72:2, 88:17
clark
78:10
class
30:11
clear
6:8, 6:12, 10:4, 18:2, 24:21, 55:2, 68:2, 70:10, 71:20, 72:11
clearly
86:21
close
37:1
code
20:4, 20:8, 20:16, 20:20, 21:2, 26:8, 27:17, 81:14, 81:18, 82:1, 82:12, 82:15, 82:18, 83:3
column
14:21, 15:4, 15:16, 16:5, 16:17, 16:18,

26:14, 31:9, 31:10, 40:20, 41:8, 42:10, 43:12, 44:15, 44:16, 54:5, 57:10, 57:16, 57:17, 77:3, 77:4, 85:6, 86:9
combination 86:13
come 17:5, 41:10, 58:10, 74:4, 77:19
comes 40:16
comfortable 71:11, 72:12
coming 39:1, 67:16
commencement 92:7
commission 93:11
common 44:8, 56:22
commonwealth 2:6, 92:3, 93:17
communicated 44:9
communication 42:1
company 38:1
compare 13:9, 14:2, 16:4
compared 13:6
comparisons 23:20
complete 71:16, 91:5
compliance 19:6, 76:8
compliant 22:19, 23:9, 87:2
comply 82:16, 82:19, 82:20, 86:16
computer 16:9, 19:4, 49:12, 63:11
concept 6:17, 9:19, 35:16, 79:7
concepts 77:19
concern 50:1, 52:21, 53:5
concerns 52:4
conducted 1:16, 2:1
confidentiality 52:5
configured 55:20
confirm 8:11
consider 70:19
considered 21:15, 25:20, 33:5, 60:20, 61:9, 69:1
consistent 14:13, 86:11, 86:12
constitute 76:11
constituted 75:20
constraints 78:5, 78:15
construction 13:5, 13:22, 17:20, 75:8, 75:10
constructions 12:7, 12:11, 73:15, 73:18, 74:2, 74:9, 74:15, 74:16, 84:19, 85:3
construed 58:20
consulting 25:11
consumer 40:4, 45:19
contact 7:15
contain 61:21
contains 51:8
content 88:16
context 9:13, 12:21, 13:13, 15:19, 18:15, 25:20, 40:18, 40:21, 43:1, 47:19, 48:19, 50:8, 54:1, 55:9, 59:1, 79:2, 79:19
contexts 9:22
continues 49:4
contrary 13:19
contrast 44:13
convention 54:1
conversion 41:13, 41:17, 44:10
convert 29:13, 33:22
converted 10:11, 34:3, 44:7
copies 8:8
copy 80:19
correct 6:6, 6:17, 8:14, 11:3, 11:21, 12:12, 12:13, 15:6, 15:10, 21:7, 21:11, 22:1, 25:3, 26:20, 27:2, 27:11, 29:14, 30:2, 32:12, 32:15, 32:18, 33:6, 34:2, 34:8, 35:9, 36:3, 38:1, 38:7, 38:10, 38:13, 39:3, 39:7, 39:11, 39:15, 41:14, 44:6, 44:21, 46:9, 47:13, 49:2, 49:6, 51:11, 53:19, 54:13, 54:16, 54:22, 55:5, 55:15, 56:1, 56:5, 56:8, 56:14, 58:13, 62:2, 71:15, 74:9, 75:1, 81:4, 82:21, 83:1, 86:2, 87:5, 87:11, 87:21, 88:4, 88:22, 91:5
corrections 91:6
correctly 85:15, 86:15
correlate 29:5
correspond 31:13
corresponding 13:6, 26:19
corresponds 31:18
could 10:14, 11:1,

11:22, 13:10, 14:12, 18:9, 18:19, 19:3, 19:4, 19:12, 22:11, 22:15, 23:16, 24:3, 24:19, 25:17, 25:19, 31:21, 34:5, 35:14, 35:18, 37:17, 43:11, 44:15, 48:10, 50:12, 51:15, 51:22, 52:6, 52:11, 53:16, 57:10, 59:1, 60:21, 60:22, 61:11, 62:5, 63:11, 66:13, 68:12, 72:18, 78:13, 81:9, 83:12, 84:13, 87:17
counsel
5:4, 7:8, 7:9, 68:12, 73:10, 73:15, 75:8, 75:16, 79:7, 79:10, 81:1, 84:16, 89:10, 92:13
counselor
73:7
couple
7:8
course
7:15
cover
52:19
covered
20:3, 20:7, 20:20, 27:16, 27:20, 81:14, 82:1
create
15:15, 18:5, 20:12, 41:5
created
16:20, 27:9
creates
29:1
creating
16:14, 16:16, 32:10
cross
59:20
cross-examination
88:7, 88:20
crossix
38:4
cryptographer
31:2
cryptographers
29:18
cryptography
18:21, 30:16, 35:17
currently
63:10

D

data
9:11, 9:18, 10:3, 10:5, 10:9, 10:16, 11:19, 18:19, 18:21, 25:8, 26:18, 38:6, 38:12, 39:10, 39:14, 41:14, 42:9, 44:5, 45:2, 46:5, 46:14, 47:2, 49:9, 54:12, 54:19, 56:11, 56:17, 57:1, 61:17, 61:21, 77:6, 79:16, 85:11, 85:20
database
42:7, 49:11, 61:6
datavant
1:5
date
32:14, 35:11, 51:8, 91:10
day
69:4, 93:9
dc
3:6
debra
1:22, 2:5, 92:2
declaration
8:17, 9:2, 9:5, 9:8, 12:3, 31:21, 39:18, 53:13, 59:7, 59:21, 61:3, 61:12, 73:20, 77:22, 79:11, 84:22, 85:4
declarations
84:18, 84:22
decode
36:17
decrypt
21:1, 21:10, 63:15, 63:19
decrypting
21:14, 64:10
decryption
22:6, 22:17, 23:14, 24:17, 24:19, 33:4, 36:12, 36:15, 36:19, 83:8
decrypts
21:1
define
46:1, 47:1
defined
17:7, 55:22
defines
18:1
definition
14:8, 14:18, 16:1, 17:11, 17:18, 17:21, 35:17, 45:20, 47:14, 47:16
definitions
41:18
deidentification
64:18, 65:17, 67:2, 69:10, 81:15, 84:8
deidentified
20:5, 27:18, 61:17, 61:21
deidentifying
10:3
depending
33:14
depends
11:7, 11:16, 18:22, 25:5
deponent
91:1
deposition
1:15, 2:1, 4:11, 7:5, 7:16, 37:20, 92:6, 92:8, 92:14, 92:16
deprecated
63:12
derivation
22:22, 81:21, 82:5, 82:19, 83:14
derive
34:5
derived
20:9, 22:22, 25:1, 26:9, 27:10, 32:19, 74:1, 81:18, 83:3
describe
29:15, 58:5
described
9:13, 16:13, 78:6, 79:19, 84:2, 86:5
describes
33:16, 33:18, 57:5
describing
41:9
descriptions
14:19
designed
86:20

details
11:14
detect
13:7, 49:18
determination
64:18, 75:3
determine
55:20
determines
45:16
device
54:12, 54:19, 56:11, 57:20
diagnoses
11:14
difference
13:3
different
15:13, 16:11, 16:13, 17:2, 17:7, 18:3, 35:14, 45:5, 47:5, 63:2, 63:9, 64:7, 64:9
direct
68:14
directed
80:16, 85:18
discern
49:10
disclose
20:14, 20:20, 21:17, 21:21, 23:3, 23:12, 24:1, 24:10, 24:17, 28:4, 28:12, 82:1, 82:3
disclosed
21:22, 22:3
discloses
23:13
disclosing
28:7
disclosure
77:5, 77:10, 85:10
discuss
10:14, 88:8, 88:11, 88:18
discussed
44:14, 56:21, 62:19, 85:6, 87:12
discusses
85:9
discussing
24:22, 29:10, 36:22, 64:20, 69:11, 87:10, 88:15
discussion
14:11, 33:1, 50:19, 75:15, 87:8
discussions
14:17, 88:16, 88:19
disease
59:4, 59:18
dissemination
77:6, 85:11, 85:19
distributed
39:10
distribution
42:17, 43:3
doctor
80:9
doctor's
11:12, 22:7, 28:22
document
19:15, 34:18, 86:16
documents
7:20
doing
22:17, 89:15
domain
19:5
done
5:17, 11:16, 12:1, 63:18, 89:14
down
12:16, 45:4, 50:14, 51:18, 55:9, 78:2
download
19:16
downloading
8:1
dr
5:6, 37:9, 62:18, 68:22, 73:12, 78:10, 84:10, 84:18, 88:6, 88:19, 89:3
duly
5:3, 92:6
during
7:15

E

e-notary
2:6, 92:2, 93:16
each
14:2, 16:19, 26:18, 32:5, 32:7, 32:12, 44:19, 45:17, 51:8
earlier
16:14, 16:15, 33:1, 62:19, 64:14
ease
14:11
easier
7:21
easiest
19:17
eastern
73:6
either
33:13, 66:5
element
77:14, 77:17
else
7:15, 22:12, 44:14, 64:7, 83:12
emailing
7:14
employed
93:3
encounters
62:1
encrypt
18:7, 21:6, 22:9, 33:13, 64:7
encrypted
12:16, 13:10, 16:8, 22:11, 26:18, 27:1, 28:20, 36:12, 63:1, 76:10, 83:17
encrypting
17:3, 39:7
encryption
12:20, 13:14, 13:18, 13:20, 14:1, 14:4, 14:5, 14:9, 14:20, 15:1, 15:6, 15:12, 15:15, 15:17, 15:20, 15:22, 16:12, 16:21, 17:2, 17:7, 17:10, 18:1, 18:3, 18:6, 18:10, 18:19, 18:20, 19:2, 19:10, 20:22, 22:8, 23:17, 25:16, 30:9, 32:4, 33:2, 33:6, 55:20, 56:5, 56:22, 63:5, 63:14, 63:17, 64:1, 75:16, 76:6
encrypts
15:22, 27:6, 64:7
end
36:7, 88:19

endeavor
5:18
ending
88:6
engine
44:20, 45:1, 45:16, 45:21, 46:5
engineering
42:18
enough
43:1, 43:6
ensures
45:19
entities
41:19, 42:2
entity
20:3, 20:7, 20:20, 26:3, 27:16, 27:20, 40:4, 40:5, 56:8, 81:14, 82:1
environment
19:1
equation
45:2
errata
91:7
erupt
36:8
esquire
3:3, 3:10
essentially
29:16, 31:18, 46:15, 47:2
est
1:18, 90:3, 92:19
even
23:22, 24:1, 82:14, 82:15, 82:18
evenheim
8:4, 36:22, 37:9, 37:18, 42:10, 42:11, 44:14
event
28:1
ever
35:13
every
5:18
examination
4:2, 5:4, 73:10, 84:16, 89:12
examined
91:3
example
11:8, 11:11, 13:11, 14:13, 15:2, 15:9, 15:16, 24:22, 26:11, 30:13, 32:4, 47:15, 50:10, 58:21, 62:11, 86:9
examples
30:15, 49:2, 51:13, 52:18, 65:21, 66:13, 66:14, 66:16, 67:15, 67:16, 67:22, 68:3, 68:6, 68:8, 68:11, 69:1, 69:17, 70:1, 70:4, 70:7, 70:11, 70:12, 70:15, 70:17, 70:19, 71:1, 71:2, 71:21, 72:8, 72:14, 72:15, 78:6
excluded
60:7
exhibit
4:11, 4:12, 4:13, 4:14, 4:15, 8:17, 8:20, 19:18, 19:19, 37:6, 37:13, 48:2, 48:3, 64:13, 80:19, 81:3, 87:11, 87:14
exhibits
4:6, 4:9, 7:19
exist
28:9
existed
87:3
exists
23:16, 24:11, 24:12, 82:8
expect
62:22, 86:17
experience
65:5
expert
64:17
expertise
69:15
expires
93:11
explain
78:13
explaining
49:15
extent
13:3, 88:15

F

facilities
62:1
fact
24:3, 78:17
factor
64:12
factors
52:4
fair
35:5, 42:8, 43:9, 43:21, 45:13, 46:16, 47:6, 49:20, 51:4, 57:3, 62:4, 62:22, 64:19, 86:7
fairly
51:19
familiar
6:17, 64:21, 86:1
far
37:22, 38:9, 38:17
fashion
76:21
faster
53:10
features
78:6
february
1:17, 92:18, 93:9
federal
77:7, 78:20, 85:12, 85:18
feel
71:11
few
38:15, 47:3, 51:12, 62:18, 79:22, 89:4
field
18:16, 18:18, 18:21
figure
37:17, 43:4, 53:3
financially
93:5
find
8:19, 35:17, 36:9
fine
5:7, 5:8, 7:21, 71:19, 73:4
first
5:9, 32:2, 39:20, 40:1
fish
3:11
fly
58:10
folder
8:6
folks
73:3
follows
5:3, 89:14

foregoing
91:4
form
18:11, 18:13, 22:4, 29:16, 46:18, 56:18, 56:19, 61:7, 82:22
formal
41:4
formed
27:1
formulated
65:18, 66:2
forth
74:6, 81:3, 82:5, 87:19, 88:3, 92:6
forty-eight
41:1
found
23:17
four
89:12
fourth
12:15, 78:2
framework
76:19, 78:21
front
7:20
full
32:2, 39:20, 40:1, 44:15
function
13:8, 13:11, 14:4, 14:6, 16:3, 16:13, 22:6, 27:7, 28:1, 28:19, 28:20, 29:1, 29:4, 29:9, 29:21, 29:22, 30:12, 30:14, 30:17, 30:18, 30:21, 30:22, 31:6, 33:10, 33:14, 33:19, 33:22, 34:16, 35:12, 35:16, 35:22, 36:5, 36:19, 36:20
functionality
14:20, 15:14, 15:21
functions
15:2, 15:8, 30:7, 30:10, 30:11, 30:13, 33:18, 34:12, 34:21, 35:2, 35:8, 35:10, 75:17
further
42:12, 45:4, 72:21, 84:11, 89:2, 90:1, 92:12, 92:16, 93:1
fuzzy
44:20

G

gave
51:12, 70:5, 76:13
general
12:19, 25:20, 35:1, 51:19, 52:5, 65:1
generally
11:18, 11:19, 15:20, 18:18, 30:20, 34:20, 47:18, 64:5, 65:5, 65:16, 69:2, 71:4
generate
40:10, 40:15, 70:17
generated
13:5
generates
16:22, 32:5, 40:5
generation
25:6
generator
16:21
getting
36:22, 69:16
give
5:10, 5:14, 47:4, 53:11, 58:21, 60:4, 62:11, 62:14, 66:9, 69:17, 70:16, 71:10, 71:15, 71:22, 72:18
given
14:9, 17:11, 17:21, 49:2, 51:14, 91:6, 92:10
giving
71:11, 72:12
go
5:8, 7:22, 8:8, 9:1, 37:14, 57:10, 62:14, 89:18, 89:21
goes
55:2
going
5:8, 14:10, 17:12, 19:14, 26:7, 30:1, 32:17, 32:22, 36:21, 38:15, 43:7, 56:10, 62:19, 63:7, 63:8, 71:18
good
5:6, 5:7, 25:16, 37:2, 70:19
great
7:2, 8:8, 14:16, 25:14, 25:15, 53:16, 54:7
ground
75:4
group
32:6, 32:7, 45:21, 46:1, 47:1, 47:9, 47:11, 54:21, 55:5, 56:12, 57:21, 58:3, 58:16, 59:4, 61:17, 62:5, 77:18
guess
11:7

H

hand
48:13, 93:9
handy
19:11, 48:8, 53:6, 66:17
happen
6:9
happens
34:10
happy
89:17
hash
13:11, 15:2, 15:8, 27:7, 28:1, 28:19, 28:20, 29:1, 29:2, 29:3, 29:8, 29:9, 29:21, 29:22, 30:7, 30:9, 30:12, 30:14, 30:18, 30:21, 31:5, 33:10, 33:14, 33:19, 33:21, 34:12, 34:15, 34:20, 35:2, 35:8, 35:10, 35:12, 35:16, 35:18, 35:21, 36:9, 75:17
head
34:19, 69:14, 69:18, 70:1
health
9:11, 9:17,

38:10, 44:19, 79:16
healthcare
10:5, 10:9, 10:16, 11:12, 11:19, 31:13, 54:20, 55:4, 55:8, 55:13, 55:19, 56:4, 56:12, 56:14, 62:1
hear
18:8, 34:22
heart
59:4, 59:18
heighten
52:4
help
41:6
helpful
34:21
helps
40:19, 40:21
here
12:6, 13:18, 14:11, 21:16, 24:8, 27:12, 30:15, 32:16, 49:16, 51:14, 54:10, 59:2, 62:5, 67:7, 67:18, 68:10, 68:22, 69:17, 69:19, 70:1, 70:3, 70:7, 71:2, 72:13, 77:10, 78:17, 84:3, 85:2, 85:21, 87:4, 87:10
hereby
91:2, 92:3
hereinbefore
92:6
hereunto
93:8
high
47:13
highlighting
8:13
hipaa
19:1, 19:2, 19:6, 19:8, 19:12, 22:18, 23:6, 26:8, 47:20, 50:8, 64:14, 65:12, 69:5, 69:10, 71:3, 76:5, 76:14, 76:16, 76:19, 77:9, 77:10, 77:20, 78:5, 78:16, 78:18, 79:1, 79:3, 81:3, 82:12, 82:20, 84:3, 84:8, 85:16, 85:17, 85:22, 86:10, 86:11, 86:12, 86:17, 86:20, 87:2, 87:3, 87:7, 87:9, 87:18, 88:4, 88:5
hipaa-compliant
76:21, 86:6, 86:19
history
50:19, 50:22, 51:7
hits
47:3
hour
5:18, 37:1
hours
89:12, 89:13
human
34:2, 34:4
hypothetical
11:7

I

id
48:22, 51:9, 83:17
idea
13:8, 19:9, 23:19, 43:18, 49:15
identical
16:22
identifiable
9:20, 17:1, 32:6, 32:11, 32:20, 38:20, 65:8
identification
20:5, 20:8, 20:21, 26:9, 27:18, 52:17, 82:2
identified
52:7, 52:11, 55:3, 55:14, 61:18
identifier
75:12
identifies
26:19
identify
10:20, 11:20, 27:2, 43:8
identifying
10:6, 10:17, 10:19, 25:2, 29:11
identities
31:14
identity
41:10, 50:9, 75:13, 77:15, 81:20
identity-disclos-ing
42:14
ignore
63:20
imperative
52:6, 52:10
implement
86:18
implemented
15:3
important
42:12
inc
1:5
include
14:3, 83:17
included
44:2
includes
48:20, 54:15
including
87:4
independently
74:1
indicate
49:18, 51:7
indicating
26:22
individual
20:10, 20:12, 26:10, 26:18, 26:19, 27:2, 27:6, 27:11, 28:19, 29:12, 32:5, 32:7, 32:12, 33:13, 42:18, 43:5, 45:19, 52:6, 52:11, 75:13, 75:14, 77:15, 81:19, 81:21
individually
65:7
individuals
31:15, 43:15, 44:2, 49:11, 54:22, 55:3, 55:21, 55:22, 56:13, 61:18, 77:18, 77:19
information
9:20, 10:6, 10:17, 10:19, 10:20, 11:5, 11:20, 13:6, 13:14, 15:22, 17:1, 20:5, 20:9, 20:11,

21:3, 21:6, 21:11, 21:14, 22:10, 22:11, 23:1, 23:21, 25:2, 25:13, 26:10, 27:1, 27:5, 27:10, 27:18, 29:11, 29:13, 32:7, 32:11, 32:15, 32:20, 33:12, 36:13, 40:11, 41:13, 48:20, 50:6, 54:16, 54:20, 55:4, 55:8, 55:13, 55:19, 56:4, 56:12, 56:14, 57:6, 57:21, 58:3, 58:16, 61:22, 63:16, 65:7, 76:10, 77:16, 81:19, 85:19
initial
42:19, 89:12
input
29:17, 30:5, 33:22, 34:5, 35:9, 63:7, 63:8, 63:19
inputs
35:14, 35:18, 36:9
instance
17:9, 27:7, 28:11, 29:11, 50:9, 65:14
instant
42:13
instruct
88:14
instructing
88:18
intended
86:16
interact
42:4
interested
41:12, 93:5
interface
38:19, 52:7, 52:12, 52:16
interfere
22:16
interpret
86:5
interpretation
24:3, 28:8, 87:18
interpretations
88:3
interpreting
76:13, 85:16
invalid
75:6
invalidate
74:14
invention
77:4, 78:22
inventions
76:17, 76:20, 80:15
inventive
78:3, 78:14
involve
16:2
involved
11:19
involves
39:6, 88:15
involving
41:17
ipr
1:11, 8:18
irreversible
33:18
issue
10:21, 13:17, 14:8, 34:9, 75:20, 80:5, 84:3
its's
16:11
itself
22:5, 82:19

J

job
1:20, 25:14, 25:15
judges
71:21
justin
3:3, 34:18, 59:6

K

keep
25:16
kept
21:9
key
13:16, 20:22, 21:1, 21:5, 21:6, 21:9, 21:13, 21:19, 22:1, 22:2, 22:5, 22:13, 22:17, 22:22, 23:9, 23:14, 23:16, 24:16, 24:17, 25:17, 33:3, 33:10, 33:14, 33:17, 33:21, 34:7, 36:11, 36:15, 36:17, 36:19, 36:20, 49:9, 62:20, 62:21, 63:2, 63:15, 64:3, 64:6
keys
33:2, 33:3, 63:7, 64:8, 64:9, 83:8
kind
69:20
knee
62:10
know
5:17, 5:20, 6:11, 7:19, 7:22, 17:19, 18:1, 23:3, 24:15, 26:3, 29:1, 33:7, 34:1, 36:5, 36:18, 53:14, 59:3, 59:17, 60:5, 61:10, 63:13, 65:12, 65:18, 66:4, 66:13, 66:17, 66:19, 67:1, 67:14, 67:22, 68:6, 68:11, 69:4, 69:13, 70:12, 70:22, 71:1, 71:2, 71:5, 71:6, 71:15, 71:18, 71:21, 72:13, 74:13, 85:21
knowledge
65:4
known
9:20, 9:22, 66:4, 67:2, 67:8, 69:4, 88:2

L

lack
25:6, 38:18
landi
8:4
landi's
83:17
language
15:4, 24:5, 24:6, 24:7, 41:5, 42:3, 42:6, 44:8, 53:22, 54:5, 56:22, 57:2, 60:18
large
43:1, 43:2
large-enough
42:15
last
9:4, 9:10,

20:13, 37:20, 52:3, 57:17, 58:7, 79:14
later
70:18
law
77:7, 85:12
laws
85:18
leading
74:22, 76:1, 80:7, 82:22, 83:5, 83:9, 83:22, 84:4
leads
76:22, 86:14
learn
50:6
least
34:2, 39:6, 45:11, 55:22, 66:14, 85:16
leave
71:19, 72:19
led
14:18
left
37:22, 38:17, 54:5
left-hand
50:13
lens
76:5, 76:14
let's
26:11, 37:2, 48:1, 62:14, 73:2, 77:2, 89:21
level
45:19, 46:8, 46:10, 46:11, 46:13, 46:14, 49:20
levels
47:19
likely
6:19, 31:5, 36:8
limitation
54:2, 54:11
limitations
60:19
limited
36:1, 36:2, 78:4, 78:14
limits
60:13, 61:5
line
15:17, 45:5, 45:15, 57:16, 57:17, 57:18, 77:4, 78:2, 86:9
lines
16:6, 16:17, 26:15, 31:8, 31:10, 40:20, 40:22, 41:8, 41:16, 42:11, 43:12, 44:15, 44:16, 45:11, 85:7
link
7:18, 64:10
linked
64:2
list
41:11, 42:15, 42:19, 42:22, 43:7, 43:18, 44:2, 44:4, 59:2, 67:5
listed
12:12
lists
38:20, 39:1, 39:7
literature
30:16
little
5:9, 37:21, 73:1
llc
1:8, 92:13
llp
3:4
log
48:20
long
23:11, 24:1, 24:7
look
9:4, 14:10, 15:16, 16:18, 17:14, 19:22, 20:1, 26:12, 26:14, 27:13, 39:17, 43:4, 48:13, 50:12, 54:3, 54:6, 54:10, 54:18, 57:5, 58:22, 61:11, 69:12, 77:3, 77:13
looked
58:4, 59:12, 59:22, 60:17, 64:14
looking
8:12, 41:7, 42:11, 64:16
looks
46:5
lot
25:10, 70:13

M

made
29:8
maintain
59:10
make
6:11, 25:17, 37:16, 46:7, 49:10, 54:9, 55:2, 57:1, 57:15, 68:18, 71:20, 72:5
makes
22:17, 56:17
making
13:14
manner
9:13, 13:18, 28:17, 49:16, 79:19, 80:4, 80:12, 86:18
manners
52:15
many
7:9, 62:10
marked
4:6, 4:9, 8:20, 19:19, 37:6, 37:12, 48:3
markings
8:12
marriage
93:3
massachusetts
3:5
match
13:7
matched
45:18, 46:7, 47:12
matches
51:9
matching
44:21
matter
23:8, 93:6
maybe
37:1, 45:16
mean
9:17, 17:10, 21:22, 23:13, 25:8, 29:19, 31:9, 35:7, 40:9, 40:14, 42:22, 64:22, 70:8, 85:16
meaning
29:21, 58:20, 75:21
meaningful
42:2
means
16:22, 18:1, 20:4, 20:8, 20:21, 21:2, 21:14, 26:9, 27:17, 36:12, 36:16, 39:13,

43:2, 43:6, 82:2, 83:13
meant 10:16, 65:1, 78:13
mechanism 20:14, 21:17, 21:20, 22:5, 22:6, 23:4, 23:12, 24:2, 24:10, 24:11, 24:12, 27:21, 28:4, 28:7, 28:13, 36:16, 82:3
medical 11:15
medication 5:13
meetings 7:8, 7:9
mention 19:7
mentioned 10:6, 20:19, 30:7
mere 22:16, 22:20, 24:3, 80:16
message 15:18, 16:7, 16:9, 18:7, 18:10, 63:20
method 22:8, 27:7, 33:6, 42:13, 49:10, 64:18
methodologies 15:2
methodology 33:15
methods 65:6, 65:17, 65:21, 65:22, 69:3, 69:7, 69:10, 78:4, 78:15
middle 38:3
might 23:17, 32:14, 53:3, 56:20, 56:21, 62:9, 62:13, 64:9, 70:19, 72:14
mind 11:8
minimum 43:15, 43:19, 44:1, 46:8, 46:10, 55:22
minneapolis 3:15
minnesota 3:15
minutes 37:3, 62:15, 73:2, 84:13
mischaracterizes 60:8
moment 17:12, 19:21, 48:5, 50:20, 53:11, 77:22, 81:9
monday 1:17, 92:18
more 6:12, 10:10, 14:22, 15:6, 21:4, 26:1, 36:7, 62:14, 62:18
morning 5:6, 5:7
most 22:8, 24:15, 26:3, 86:1
much 62:14
murphy 48:1, 48:11, 49:15, 51:15
must 25:20, 42:22
mutually 41:18

N

name 11:1, 29:2, 29:12, 30:1, 32:14, 45:21, 63:1, 64:1, 64:7, 64:8
naming 54:1
narrowing 50:3
nature 61:5
need 5:19, 8:7, 8:9, 19:21, 24:1, 28:6, 29:3, 36:17, 36:18, 36:20
network 16:9
never 22:2, 23:13
new 58:6, 58:9, 67:19, 72:5, 72:7
next 49:8, 77:17
nicholas 3:10
none 4:7
nonetheless 78:5
nos 1:12
notes 7:12, 8:13
notice 2:5
nsa 22:15
number 11:2, 25:6, 34:13, 35:3, 35:8, 36:1, 36:2, 36:6, 43:15, 43:20, 44:1, 45:17, 46:5, 49:1, 50:2, 51:9, 54:21, 55:21, 55:22, 56:13, 59:3, 59:17, 62:6, 81:2
numbered 48:14
numbers 50:15
nw 3:5

O

oath 66:9
obfuscation 49:10
object 6:4
objection 18:13, 22:4, 46:18, 58:17, 59:5, 59:11, 59:19, 60:15, 61:7, 67:11, 68:18, 68:20, 69:8, 71:8, 74:22, 76:1, 80:7, 82:22, 83:5, 83:9, 83:19, 83:22, 84:4, 88:13
objections 68:16
obtained 16:19
obvious 74:21
obviousness 78:8
occurred 92:17
occurs 17:14

october
93:11
offer
72:9, 83:11, 83:16
offered
15:8, 59:21
offering
12:11, 85:2
office
1:1, 11:13, 22:7, 28:22
often
6:14
oh
9:6, 57:7
okay
6:13, 8:22, 9:3, 9:9, 12:4, 19:14, 19:21, 25:4, 26:13, 26:16, 27:15, 30:7, 31:11, 32:1, 36:11, 37:11, 37:19, 39:19, 40:1, 40:12, 42:10, 43:13, 44:17, 46:12, 46:20, 48:1, 48:8, 48:12, 50:21, 51:16, 52:2, 53:18, 53:20, 54:8, 55:11, 57:7, 57:9, 57:11, 57:14, 61:13, 61:15, 65:2, 67:20, 72:4, 73:7, 78:1, 80:22, 81:11, 89:19
oliver
3:3, 4:3, 5:5, 34:19, 36:21, 37:8, 37:12, 59:8, 62:13, 62:17, 68:15, 72:21, 73:4, 73:8, 74:22, 76:1, 80:7, 82:22, 83:5, 83:9, 83:19, 83:22, 84:4, 84:12, 84:17, 88:17, 89:1, 89:5, 89:8, 89:10, 89:19
on-the-fly
60:4, 66:20, 70:16, 70:17
once
64:11
one
5:20, 12:15, 13:7, 14:15, 14:22, 15:6, 15:9, 15:13, 16:13, 17:8, 18:5, 18:9, 18:19, 21:4, 21:6, 23:1, 23:13, 23:16, 23:22, 28:18, 29:15, 31:18, 31:19, 33:11, 34:4, 34:6, 34:11, 43:8, 48:6, 48:15, 52:20, 53:2, 56:18, 56:19, 60:10, 62:22, 67:5, 68:18, 81:22, 85:22, 86:4, 86:21
one-way
30:12, 30:13, 30:14, 30:17, 30:20
one-word
68:16
ones
29:8, 87:8, 87:12
only
19:9, 21:22, 24:21, 33:18, 34:7, 36:2, 52:20, 53:2, 78:18, 83:7
open
8:2, 8:4, 8:5, 8:16, 8:22, 48:6, 48:8
opened
14:15
opening
53:12
operate
78:4, 78:15
operating
19:1
operation
34:15, 62:1, 62:7
operations
76:20
opinion
58:6, 58:9, 65:19, 66:3, 66:10, 74:8, 76:22, 77:12, 83:11, 83:16
opinions
60:4, 70:17, 72:7, 74:17, 74:19
option
33:10, 61:1
order
42:1, 42:5
ordinary
6:16, 6:20, 31:3, 33:5, 52:14, 58:19, 65:11, 65:15, 65:22, 66:7, 69:3, 86:17, 86:22, 87:15, 87:20, 88:1
organizations
25:22
original
10:12, 29:4
other
8:6, 9:11, 11:14, 13:15, 14:2, 15:2, 15:16, 16:22, 20:4, 20:8, 20:21, 21:2, 21:19, 23:1, 26:8, 27:17, 30:8, 30:9, 30:15, 30:17, 32:15, 33:11, 34:9, 58:20, 60:10, 60:18, 79:17, 80:11, 82:2, 82:3, 85:18
others
8:3, 22:15, 26:1, 26:5
otherwise
7:2, 7:14, 93:5
out
12:22, 15:5, 16:6, 23:17, 26:7, 43:4, 53:3, 65:13, 69:22, 71:12, 72:9, 72:16
outcome
93:6
output
30:2, 30:4, 34:1, 34:3, 34:5, 34:6, 34:14, 35:4, 35:15, 35:18, 35:20, 36:10, 63:2, 63:8
outputs
36:3, 36:4
outside
12:22, 13:12, 14:5, 33:8, 64:5, 78:19
over
16:8, 37:14
own
84:20
owner
1:9, 3:9,

73:10, 90:1

P

p-o-s-a
6:21
page
4:2, 4:11, 20:1, 32:3, 37:22, 39:21, 40:2, 48:10, 50:12, 51:10, 51:15, 53:17, 54:10, 54:12, 57:18
pages
1:21
papers
34:11
paragraph
9:1, 9:5, 12:2, 12:5, 12:12, 12:15, 31:7, 31:22, 32:3, 39:17, 45:4, 45:11, 49:2, 49:8, 50:14, 50:18, 51:10, 51:12, 51:18, 51:22, 61:14, 73:20, 77:21, 79:11, 79:15
paragraphs
48:14, 54:6
parameter
44:2, 44:4
parameters
50:3
part
20:13, 21:16, 21:21, 28:16, 42:14, 63:20
participants
45:17, 45:18, 47:12
particles
36:6
particular
9:13, 10:20, 11:12, 11:17, 34:18, 43:4, 48:22, 50:9, 52:17, 62:6, 67:3, 79:18
parties
17:20, 25:9, 93:2, 93:4
party
32:4, 92:12
past
10:1
patent
1:1, 1:3, 1:9, 1:12, 3:9, 7:6, 8:3, 8:17, 9:12, 9:14, 12:22, 13:13, 14:10, 14:12, 15:13, 17:6, 17:10, 17:13, 17:14, 17:22, 18:4, 18:15, 18:17, 26:12, 26:15, 27:4, 27:10, 31:8, 31:22, 32:17, 33:8, 33:16, 53:7, 53:22, 54:11, 57:5, 57:8, 57:16, 61:5, 65:14, 69:5, 73:10, 77:2, 77:8, 78:7, 79:18, 79:19, 85:6, 86:4, 86:9, 86:10, 86:20, 87:1, 87:5, 90:1
patents
7:7, 8:5, 8:6, 13:17, 13:21, 14:3, 14:7, 55:16, 65:13, 75:6, 75:19, 75:21, 76:4, 76:8, 76:18, 79:4, 80:5, 80:13, 80:16, 84:2, 87:4
patient
10:21, 11:20, 22:12, 38:20, 39:1, 39:7, 52:4, 52:17, 52:21
patient's
50:9
patient-identifying
22:9, 22:11
patients
41:11, 49:1, 51:9, 59:2, 59:3, 61:22
pattern
49:11
patterns
49:18
pbms
38:10
pc
3:11
pdf
53:18
pending
5:21
people
43:7, 43:20, 46:6, 46:7, 53:2, 53:4, 59:17, 62:6, 62:10, 64:7, 86:1
percentage
45:18, 46:7, 47:12
perfectly
26:6
perform
46:15, 51:2, 66:19, 74:13
performed
49:17
permitted
68:17
person
6:15, 6:20, 23:13, 30:20, 31:3, 31:19, 33:5, 33:15, 52:14, 64:2, 64:8, 65:4, 65:11, 65:15, 65:22, 66:7, 69:3, 86:4, 86:17, 87:15, 87:20, 88:1
person's
11:11, 30:1, 52:13
personal
27:5, 33:12, 77:6, 85:11, 85:19, 85:20
personally
9:19, 10:6, 17:1, 32:6, 32:11, 32:20, 76:7
persons
31:13
perspective
6:15, 7:3
pertain
81:12
petition
53:6, 53:17, 54:2, 54:11, 57:13, 73:19, 74:6, 75:11, 78:8
petitioner
1:6, 3:2, 5:4, 12:7, 74:5, 75:11, 78:9, 84:16
petitioner's
73:14, 74:15, 75:7, 75:16, 79:7, 79:10, 81:1
petitions
74:20, 75:4

ph
1:15, 2:1, 4:2, 5:2, 91:2, 92:5, 92:17
pharmaceutical
38:1
phi
76:7
piece
36:13
pii
75:20, 83:3
place
16:15, 17:6, 17:9, 17:17, 39:14, 76:21
plain
58:19
plan
44:19
plans
38:10
play
76:17
plaza
3:12
please
5:20, 6:11, 7:3, 18:8, 21:4, 31:22, 37:10, 40:12, 44:16, 45:22, 46:22, 48:2, 52:1, 53:11, 59:17, 66:15, 68:17, 72:3, 81:9, 87:17, 89:22
point
5:19, 43:11, 87:19
pointed
15:5, 16:5, 26:7, 78:21
portion
57:19, 59:6, 63:21, 68:13
posa
6:21, 10:8, 18:9, 50:4, 52:21
posa's
7:3, 12:19
posed
6:6, 66:22
position
38:3, 86:3
position's
56:8
possibility
22:16, 22:20, 23:5
possible
22:9, 26:2, 27:22, 28:11, 35:8, 36:3
post
61:22
posture
25:5
practice
86:22
pre
61:22
pre-pending
63:18
preagreed-upon
42:3
preclude
59:16, 60:3, 61:1
predetermined
43:15
preparation
17:16
prepare
7:5, 69:20, 73:2
prepared
61:2, 66:11, 67:6, 67:22, 68:7, 70:16, 70:20, 72:9
present
42:16, 43:2, 77:5, 85:9
presumes
56:16
pretty
18:2
previously
8:20, 19:19, 37:6, 48:3
primarily
87:8
principle
67:3
principles
65:6, 65:16, 65:20, 65:22, 66:6, 67:1, 67:8, 69:2, 71:4
prior
4:9, 7:7, 9:12, 16:8, 65:13, 69:4, 74:13, 74:20, 75:5, 78:7, 79:17, 80:2, 80:3, 87:3
privacy
19:12, 20:18, 26:8, 45:19, 45:22, 46:22, 47:8, 47:10, 47:22, 52:13, 64:14, 81:3, 81:7
private
21:5, 21:10, 21:13, 21:22, 22:2, 33:1, 36:15, 36:17, 36:20, 50:7, 63:15, 64:6, 64:8
privilege
6:5
privileged
88:13
probably
31:2, 53:9, 85:22
problem
28:14, 48:7, 62:12
problematic
23:15
proceeding
73:16
proceedings
80:3
process
8:1, 23:7
processing
42:15, 77:5, 85:10
processor
40:3
processors
40:4, 40:6
produce
14:22
produced
77:16
producing
54:20, 56:11, 77:14
professional
31:1
program
19:3, 45:6, 45:7, 45:17, 46:6, 48:21, 49:4, 63:11
programs
45:6, 45:12
prohibited
24:4
prominently
78:6
proper
43:20
protect
42:17, 52:13
protected
25:9, 25:13
protecting
47:21
provide
7:18, 66:10, 68:4, 70:11, 72:2, 72:7, 84:19
provided
16:2, 20:7,

27:20, 73:19, 75:11, 85:3
providers 31:14
provides 28:17
providing 84:21
provision 81:12, 82:5, 82:9
provisions 81:2, 81:16, 81:17, 82:11, 83:4, 83:20
public 2:6, 21:5, 33:1, 33:14, 36:19, 63:1, 92:2, 93:16
public-private 24:16, 33:3, 33:10, 33:17, 33:21, 36:11, 62:20, 62:21, 63:6
purpose 33:17, 82:3
purposes 9:12, 79:17
pursuant 2:5
put 19:14, 19:15, 29:2, 53:7, 53:10
putting 19:18, 50:2

Q

qualify 20:13, 70:4, 71:3
queries 40:3, 40:4, 41:5, 51:3, 52:20
query 39:7, 39:9, 39:13, 42:15, 42:16, 42:19, 44:20, 45:1, 45:16, 45:21, 46:4, 49:1, 50:2, 50:3, 51:8, 52:5, 53:1, 61:5
question 5:21, 6:10, 17:13, 21:15, 24:14, 33:20, 34:22, 35:1, 40:13, 40:20, 59:12, 60:20, 61:9, 64:4, 66:9, 68:2, 72:6, 72:10, 88:15
questions 6:4, 6:6, 6:8, 6:14, 7:4, 41:6, 61:2, 62:18, 66:22, 67:18, 68:19, 72:21, 79:22, 81:2, 81:6, 84:11, 89:2, 89:4, 89:16, 90:1
quick 54:3

R

raised 74:20
random 25:6, 63:18, 64:11
randomized 63:5, 63:14, 63:17
rather 54:7
rbc 3:12
read 34:11, 44:16, 50:18, 50:20, 59:15, 60:1, 60:13, 60:22, 81:9, 91:3
readable 34:1, 34:4
reading 40:17, 87:16, 88:5
reason 5:10, 6:9, 22:13, 25:10, 29:20, 47:18
recall 64:20, 73:14, 73:21, 75:7, 75:15, 79:6, 79:12, 79:20, 81:6, 84:21
received 11:15
receives 40:3
receiving 57:20
recess 37:5, 62:16, 73:9, 84:15, 89:9, 89:20
recognizable 49:11
reconstituted 29:16
record 10:12, 11:5, 11:12, 20:4, 20:8, 20:21, 22:10, 26:9, 27:17, 34:12, 37:13, 51:2, 62:14, 68:2, 70:8, 71:20, 82:2, 84:13, 89:18, 89:21, 90:3, 92:9
records 38:13, 52:21, 53:2
recovery 23:20
recreate 29:3
redirect 73:1, 84:12, 88:7, 88:21
refer 6:19, 14:14, 61:16
reference 10:14, 37:10, 41:17, 43:14, 44:19, 45:5, 48:2, 62:4, 65:4
referenced 45:10, 79:10, 79:14
references 7:7, 74:14, 75:5, 80:4
referred 38:4, 38:10, 51:1
referring 24:6, 31:5, 32:10, 34:17, 41:22, 44:10, 45:14, 47:11, 57:4, 59:7, 78:17, 78:19
refers 15:5, 38:19, 49:5, 54:12
regard 35:7, 76:17, 80:1
regarding 61:22
regular 13:19
regulated 19:1
regulation 19:8
reidentification 20:15, 20:17, 21:18, 21:20, 23:2, 23:4, 23:5, 23:12,

24:2, 24:10, 28:5, 28:8, 28:11, 28:13, 28:18, 81:13, 82:4, 82:12, 82:15, 82:18, 83:3, 83:13, 83:21
reidentified 20:6, 24:4, 27:19
reidentify 21:2, 22:12, 23:7, 28:18
reidentifying 21:14, 27:22
relate 77:10
related 20:9, 26:10, 81:6, 81:19, 93:1
relates 77:5, 85:10
relating 11:15
relative 6:15, 10:12, 29:2
released 67:9, 69:6, 88:4
releases 22:10
relevant 87:7
relied 12:7, 12:9
relying 19:8, 20:18, 21:16
remain 11:6, 11:10
remains 10:12, 11:13
removed 10:7
removing 11:19
render 24:5, 74:8, 74:21, 75:6
rendering 65:7, 74:17
repeat 40:12, 70:9, 80:8
repeated 18:8
repeatedly 50:2
rephrase 17:15, 63:22, 75:2, 87:9
replacing 9:19, 10:17, 57:5
report 8:2, 52:19, 58:4, 61:10, 66:12, 67:18, 68:14, 69:21, 70:2, 70:14, 71:14, 72:17
reported 1:22
reports 7:6, 8:6, 70:14
represent 26:18
represented 92:13
represents 27:3
reproduced 73:19
reproducible 29:21
request 14:22, 15:18, 16:7, 16:9, 26:17, 32:5, 47:5, 55:3, 55:7, 55:12, 55:14, 55:19, 55:21, 56:3, 56:4, 56:13, 56:16, 57:20, 59:1, 59:16, 60:14, 62:9
requests 40:5, 40:10, 40:15, 61:16
require 67:17, 68:8
required 6:5, 19:6, 82:11, 82:13, 87:14
requirement 82:14, 82:16, 82:19
requirements 83:15, 84:7
reread 7:6
research 69:13
researched 69:22, 71:12, 72:16
researcher 41:7
respect 19:7, 62:20, 66:5
responds 45:21
response 80:8, 89:13
rest 86:10
restricted 77:7, 85:12
result 34:13, 35:14, 42:18
resulting 29:14
results 42:16, 43:4, 43:8, 47:4
return 52:20, 73:6
returned 49:1, 51:9
returns 53:2
reveal 31:14, 75:13
reverse 14:4, 23:7, 36:14, 42:17
reversed 14:6
reversible 16:3, 19:2, 20:16, 20:22, 30:8, 30:10, 75:16, 76:6, 76:9, 84:9
reversibly-encrypted 75:20, 83:2
review 32:17, 43:22, 51:22, 58:12, 75:19, 80:2
richardson 3:11
right 6:1, 6:22, 9:21, 10:22, 14:15, 16:6, 21:8, 24:22, 27:12, 31:11, 36:4, 38:9, 38:15, 39:17, 44:13, 48:10, 48:13, 50:11, 53:16, 54:9, 55:7, 55:18, 56:3, 62:13, 68:4, 71:2, 72:19, 72:22, 73:3, 77:2, 85:5, 85:17
right-hand 51:17
risk 24:18, 25:18, 50:4
robust 24:16

role
76:16
round
89:16
rubin
1:15, 2:1, 4:2, 5:2, 5:6, 37:9, 62:18, 68:22, 73:12, 84:10, 84:18, 88:6, 88:19, 89:3, 91:2, 92:5, 92:17
rule
19:12, 20:18, 22:21, 23:19, 27:14, 28:6, 28:10, 69:11, 71:3, 81:3, 81:7, 89:11
rules
25:10, 26:8, 64:14, 67:9, 84:8, 87:3, 87:7, 87:9, 87:14, 87:16, 87:19, 88:4, 88:5
running
48:21
runs
44:20

S

safe
30:19
safeguard
47:10
safeguards
45:22, 46:22, 47:8
said
9:6, 58:8, 66:17, 67:10, 67:13, 68:5, 71:17, 80:10
sake
6:19
same
12:6, 16:12, 16:20, 17:1, 18:5, 18:10, 29:22, 30:1, 35:15, 35:18, 36:10, 37:22, 43:18, 50:2, 51:13, 54:10, 57:2, 63:1, 63:3, 63:7, 63:8, 64:1, 64:11, 66:2, 70:5, 80:12, 91:4
satisfies
13:9
satisfy
83:4, 83:14, 84:7
saw
17:17
say
9:7, 12:6, 22:20, 25:19, 28:6, 30:19, 37:2, 39:21, 46:10, 51:5, 56:19, 59:22, 60:5, 60:6, 60:10, 62:22, 66:16, 87:17
saying
29:20, 41:4, 43:10, 46:4, 47:7, 54:19, 68:3, 68:7
says
9:10, 14:21, 16:7, 17:10, 18:19, 20:3, 20:7, 20:14, 21:17, 23:3, 23:11, 24:9, 27:16, 28:4, 28:12, 30:20, 44:19, 45:16, 46:11, 46:14, 46:19, 46:21, 55:18, 77:4, 81:22, 86:16
scientific
65:6, 65:20, 65:21, 66:6, 67:1, 67:8, 69:2, 71:4
scope
18:13, 58:2, 58:5, 58:12, 58:18, 59:9, 59:11, 59:20, 60:7, 60:12, 60:16, 61:8, 67:12, 68:21, 69:9, 71:9, 83:19
search
40:5, 40:10, 40:15, 42:5, 46:15, 47:3
searched
38:13, 46:6, 54:16
searches
49:16
searching
39:14, 43:19
second
8:19, 12:5, 21:9, 21:16, 21:21, 48:15, 77:14
secret
25:17
section
20:6, 20:18, 27:13, 27:19, 31:12, 37:22, 38:17, 64:16
sections
54:7
secure
22:8
secured
26:6
securely
26:4
security
11:2, 25:5, 26:1, 34:9, 81:22, 82:8, 82:14, 82:16, 83:14
see
9:15, 12:8, 12:17, 13:4, 24:6, 24:7, 27:12, 29:19, 31:16, 32:8, 38:21, 40:7, 40:8, 41:20, 42:20, 43:16, 45:8, 46:2, 46:5, 48:16, 49:13, 49:17, 50:16, 51:20, 52:8, 57:22, 58:5, 58:22, 60:2, 60:22, 61:19, 62:12, 65:9, 70:8, 78:11, 85:13
seem
24:4
seems
41:9, 46:4, 50:22, 55:13, 56:10
seen
25:11
sending
15:17, 39:13, 41:13
sense
32:19, 49:9, 58:15
sent
39:2, 44:3, 44:4, 44:5, 55:19, 56:4
sentence
9:4, 9:10, 12:5, 32:2, 39:20, 40:2, 52:3, 78:2,

79:15
server
14:20, 15:15, 15:22, 16:21, 32:4, 54:12, 54:15, 54:19, 55:20, 56:5, 56:11, 56:17, 56:22, 57:1
session
4:6
sessions
4:9
set
34:13, 35:3, 35:8, 74:6, 81:3, 82:5, 87:19, 92:6, 93:8
settimi
8:4
setting
88:3
seven
89:12
several
14:17, 70:14
share
19:12, 66:14
shared
41:17
sheet
91:7
short
37:2, 89:5
should
15:12
show
10:13, 19:12
shown
87:10, 87:14
side
45:2, 50:13, 51:17
sides
13:22
signature
91:10
signature-p1kal
93:14
signed
91:7
similar
11:2, 18:20, 56:8, 56:20
similarly
12:16, 13:10
simple
57:15
simplicity
6:19
simply
15:5, 41:2
since
5:17, 36:22
single
52:6, 52:10
sit
30:15
sites
16:20
sitting
67:7, 68:10, 68:22, 69:18, 70:1, 70:3, 70:7, 71:2, 72:13, 85:21
size
35:19, 47:11
skill
6:16, 6:20, 31:3, 33:5, 52:14, 65:11, 65:15, 66:1, 66:7, 69:3, 86:18, 86:22, 87:15, 87:20, 88:1
small
24:19, 25:18
social
11:1
some
5:19, 9:21, 27:6, 29:11, 34:9, 37:14, 41:12, 42:3, 49:16, 49:19, 52:15, 53:21, 56:8, 56:18, 56:21, 60:19, 63:18, 65:21, 66:10, 66:13, 66:14, 67:15, 67:17, 68:9, 69:12, 78:20, 84:12
somebody
43:3, 64:6
someone
13:15, 22:12, 24:15, 24:19, 25:12, 25:21, 64:6
something
11:2, 26:4, 44:14, 62:19, 63:11, 66:18, 67:17, 67:21, 68:8, 69:13, 69:14, 70:15, 78:19
sorry
9:6, 9:7, 16:5, 24:9, 30:12, 31:10, 39:21, 40:17, 57:15, 58:7, 64:22, 68:15, 80:8
sort
28:3, 41:12, 49:4, 49:19, 58:11
source
16:19, 25:6, 40:5, 41:19, 42:2, 45:2, 46:5, 46:14, 47:2
sources
38:12, 39:10, 39:14, 41:14, 42:9, 44:5
south
3:13
speak
85:1
speaking
11:18, 30:20, 57:1, 68:16
specific
10:10, 11:8, 14:8, 17:18, 19:8, 41:6, 67:8, 68:13, 80:17, 84:19
specifically
10:2, 10:13, 31:8, 46:21, 54:2, 79:14
specification
77:9, 78:7, 86:11
specifics
11:14, 41:10, 42:14
specifying
7:2
spontaneously
36:8
standard
23:10, 25:21, 35:10, 63:4
standards
63:12
start
36:5, 44:18, 88:20
starting
45:15
stated
41:2
statement
86:3
statements
86:8, 86:13
states
1:1, 26:17, 31:12, 32:3, 40:2, 42:11, 49:8, 52:3, 55:12, 57:20, 60:13, 78:18,

78:20, 78:22, 79:3, 79:15
statistical 42:17, 43:3, 45:20, 47:14, 47:16, 65:6, 65:16, 66:5
stay 57:12
staying 42:10
step 38:18, 39:6, 39:9
stephens 3:10, 4:4, 18:13, 22:4, 34:17, 46:18, 58:17, 59:5, 59:10, 59:19, 60:8, 60:15, 61:7, 67:11, 68:12, 68:20, 69:8, 71:8, 72:22, 73:5, 73:11, 84:10, 88:7, 88:9, 88:12, 88:13, 88:22, 89:3, 89:7, 89:17, 89:21
steps 39:6
stick 57:16
sticking 15:4
still 6:5
street 3:13
strength 35:21
strike 82:16, 83:11
subection 82:6
submitted 70:14
subsection 81:7, 81:10, 82:9, 83:4, 83:7, 83:12, 83:20
substance 88:8
successful 42:6
sufficient 42:16
suggesting 28:14
suite 3:14
superfluous 24:5
supports 77:12
suppose 11:10
supposed 50:7, 66:19, 66:21
sure 8:2, 10:2, 10:13, 18:9, 21:5, 24:13, 28:13, 29:18, 37:4, 37:16, 40:14, 45:14, 46:7, 47:17, 53:11, 54:9, 56:9, 57:1, 67:7, 71:15, 87:18, 89:7, 89:15
surgery 62:10
switch 36:21
sworn 5:3, 92:7
system 11:17, 20:22, 21:5, 21:13, 24:16, 25:16, 33:17, 33:21, 36:11, 62:22
systems 33:22, 34:3, 62:20, 63:4, 63:6, 63:10, 63:13, 78:4, 78:14

T

table 50:19, 50:22, 51:7, 73:18, 74:2, 74:17
take 5:18, 5:22, 17:12, 26:11, 29:11, 33:12, 33:22, 39:14, 48:7, 50:12, 50:20, 54:3, 54:6, 58:19, 58:21, 59:14, 60:12, 73:2, 76:20, 81:9, 89:5
taken 37:5, 62:16, 73:9, 84:15, 89:9, 89:20, 92:8
takes 27:5, 41:10
taking 5:13
talk 34:20, 40:20, 53:21, 55:8
talked 16:16, 37:20, 51:10
talking 15:17, 15:19, 15:21, 18:14, 18:18, 25:3, 30:21, 33:7, 33:9, 45:1, 55:14, 64:5, 65:14, 87:4
talks 16:14, 16:15, 22:21, 44:1, 77:9, 77:15, 77:17, 86:10
targeted 25:7
technique 18:6, 18:20, 24:20
techniques 15:1, 15:6, 22:14, 30:9, 80:16
technology 78:3, 78:14
tell 67:14, 71:5
telling 47:2
tempest 22:15
ten 37:2, 62:15
tend 35:11
tension 27:12
term 10:4, 13:18, 13:19, 17:7, 38:19
terms 12:12, 12:14
testified 5:3
testimony 5:11, 5:15, 59:20, 60:9, 76:12, 88:8, 91:4, 91:6, 92:9
texting 7:14
th 93:9
thank 5:8, 57:7, 73:13, 84:10,

89:8
themselves
85:1
theoretical
30:16
theoretically
35:14
theories
72:5
theory
21:10
therefore
47:4
thing
58:7, 64:11, 69:20
things
5:9, 13:9, 14:2, 36:5, 38:16, 69:21, 70:2, 70:13, 71:13
think
10:5, 14:17, 17:19, 18:2, 18:22, 22:14, 25:4, 25:9, 25:19, 26:4, 26:5, 27:13, 31:1, 32:18, 33:16, 37:15, 37:20, 43:10, 52:18, 53:9, 64:17, 67:4, 67:16, 69:16, 71:10, 72:22, 85:22
thinking
30:15
thinks
25:12
third
32:3
thought
9:6, 66:10, 69:22, 70:18, 71:12, 72:8, 72:16
thoughts
58:22
three
54:6, 84:13, 89:14
threw
64:11
through
5:9, 8:1, 16:6, 19:22, 31:8, 31:10, 38:15, 40:21, 40:22, 41:9, 42:11, 44:7, 44:16, 45:11, 52:7, 52:11, 52:16, 54:3, 58:4, 76:4, 76:14, 85:7
throughout
77:8, 86:8
time
21:4, 37:2, 48:7, 48:22, 51:8, 59:14, 60:13, 65:12, 66:1, 66:5, 67:2, 67:9, 69:5, 73:1, 87:16
times
25:11, 63:2, 63:9
today
5:11, 6:14, 14:12, 17:16, 63:4, 63:13, 64:22, 65:14, 67:7, 68:11, 68:22, 69:17, 69:19, 70:3, 71:2, 72:13, 85:2, 87:4, 87:10
today's
4:6
together
29:7, 64:2
token
9:20, 10:11, 10:18, 16:19, 16:20, 16:22, 18:5, 18:11, 20:12, 23:21, 25:1, 26:17, 26:22, 27:9, 29:14, 31:18, 32:5, 32:10, 32:19, 75:8, 75:10, 75:21, 76:9, 76:11
tokenization
11:6, 11:13, 11:18, 12:1, 17:8, 22:18, 23:8, 27:5, 29:10, 79:8, 80:12, 80:16, 80:18
tokenize
10:9, 11:9, 11:17, 18:20, 33:11
tokenized
9:11, 9:17, 79:16
tokenizing
10:5, 10:16
tokens
13:5, 14:22, 15:15, 16:1, 16:14, 16:16, 19:3, 31:12, 57:6, 80:4, 83:21, 84:2
tool
52:5
top
14:21, 16:17, 32:3, 34:19, 39:20, 40:2, 49:20, 69:13, 69:18, 69:22
towards
48:13
tracks
49:16
trademark
1:1
trail
48:15, 48:19, 49:5, 51:2, 51:6
transcription
91:5
transfer
8:9
transform
36:14
translated
81:20
transmission
17:3, 17:4, 17:9, 18:7, 18:11, 18:19
transmitted
16:8
transmitting
77:6, 85:10
treated
31:13, 31:15
treatment
11:15
trial
1:3
true
31:2, 91:4, 92:9
truthful
5:11, 5:14
try
6:8, 6:11, 46:1, 46:22, 47:5, 58:10
trying
68:1, 70:21, 71:20, 72:6
turn
12:2, 31:7, 31:21, 37:9, 37:17, 43:11, 48:1, 48:10, 51:15, 53:16, 55:9, 57:8, 64:13, 77:1, 77:22, 85:7

twice
64:1
two
7:11, 7:12, 15:13, 17:7, 18:3, 23:17, 29:6, 35:13, 35:18, 36:4, 36:9, 52:4, 52:20, 53:2, 63:2, 64:7, 81:15, 81:17, 89:13
two-minute
89:6
two-thirds
50:13, 51:18
type
15:20, 16:11, 17:2, 18:6, 18:10, 22:18, 33:6
types
19:9
typical
34:15, 62:21
typically
10:9, 11:6, 30:21, 34:12, 35:3, 56:7, 63:17

U

uh-huh
20:2
ultimate
75:3
ultimately
44:5, 56:17, 74:19
unattainable
77:16
under
20:1, 20:6, 20:19, 24:2, 27:19, 28:8, 28:12, 65:3, 66:9, 69:10, 71:3, 82:12, 83:4
understand
6:3, 6:10, 13:17, 28:14, 50:4, 52:15, 58:11, 65:15, 68:1, 71:7
understanding
10:16, 11:22, 12:20, 13:19, 23:6, 27:4, 35:2, 48:18, 55:16, 58:2, 64:4, 85:15, 86:2, 86:15, 89:11
understands
42:7
understood
15:20, 57:7, 65:12, 87:15
unencrypted
16:10
united
1:1, 78:18, 78:20, 78:22, 79:3
universe
36:6
unreadable
13:15
up-to-date
22:8
uploaded
7:18, 39:2
uploads
38:20
usage
10:8
use
7:3, 12:6, 14:12, 18:9, 20:11, 20:20, 21:6, 25:16, 33:15, 42:4, 42:6, 56:21, 63:5, 63:13, 63:14, 80:4, 82:1, 82:12, 84:13
user
25:2, 38:17, 38:19, 39:2, 40:11, 40:16, 41:11, 41:12, 47:3, 47:21, 48:22, 49:17, 50:1, 50:5, 51:3, 51:8, 51:19, 52:7, 52:11, 52:16, 53:3, 56:7, 57:20, 59:16
user's
60:14
user-identifiable
57:6
users
46:1, 47:1, 47:9
uses
18:3, 22:8, 24:15, 29:22
using
13:13, 13:18, 13:22, 16:1, 16:12, 16:20, 16:21, 18:5, 21:19, 27:6, 28:19, 28:20, 32:4, 33:11, 33:13, 33:16, 33:18, 33:21, 47:19, 52:5, 80:18
utilized
15:1

V

valid
82:12
value
63:18
variable
41:18
vary
35:11
venable
3:4
versions
8:12
view
87:19
viewed
79:16
vigilytics
1:8, 92:13
violate
84:3
virginia
2:7, 92:3, 93:17
virtually
1:16, 2:2, 92:9, 92:17

W

want
37:14, 37:16, 50:18, 53:22, 54:3, 54:5, 54:9, 55:8, 60:4, 70:16, 70:22, 71:1, 72:7
wants
33:15, 47:8
washington
3:6
way
18:1, 27:9, 29:15, 50:13, 51:18, 58:20, 60:10, 76:10, 80:17, 87:1, 93:5
ways
15:13, 17:8, 30:17
we'll
8:8, 57:15
we're
10:4, 13:13,

14:13, 24:21, 29:10, 33:7, 33:9, 36:22, 37:21, 45:1, 54:10, 64:4, 69:11, 69:16, 87:4
we've 5:17, 64:17, 65:13, 89:14
website 45:6
welcome 73:12
well-funded 26:3
weren't 70:19
whatever 11:9
whereas 14:5, 15:21
wherein 55:12
whereof 93:8
whether 18:22, 33:9, 45:17, 60:17, 67:4, 68:10, 70:10, 71:1, 71:21, 72:12, 72:13, 74:8
whitehead 1:22, 2:5, 92:2
whole 8:1, 17:14, 35:16
willing 70:11, 71:14, 71:18, 71:19, 71:22, 72:1, 72:4, 72:5
within 12:21, 14:2, 18:14, 19:7, 22:13, 34:11, 38:17, 39:5, 59:1, 59:3, 60:12, 69:14, 75:21, 76:8, 78:5, 78:15, 78:22, 85:17
without 22:12
witness 37:4, 78:9, 88:14, 88:18, 90:2, 92:5, 92:10, 93:8
witness's 60:9
word 15:12, 16:12, 68:18
words 17:22
work 55:17, 67:17, 68:9
worked 66:18
working 19:5
world 12:22, 13:12, 36:8, 64:5
wouldn't 19:5, 28:2
writing 25:21
written 76:4

Y

yeah 12:9, 12:10, 13:4, 19:17, 35:10, 46:17, 49:22, 57:19, 60:21, 64:22

.

.1 26:7
.2 20:19, 24:9

0

00307 8:18
00311 1:11
00381 1:11
00382 1:11
012 8:2, 8:5, 76:18

1

10,109,375 1:12
10,886,012 1:13
100 59:2, 59:17
1005 4:12, 37:6, 37:13
1009 4:13, 48:2, 48:3
11 73:6
12 31:8, 31:10, 57:10, 57:16, 57:17, 90:3, 92:18
13 42:11, 43:12
16 44:15, 44:16, 53:17, 54:12
160 35:11, 36:4, 36:5
164.514 64:16
17 1:17, 92:18
18 42:11, 45:5
19 4:15

2

2-5 16:17
20 73:2, 93:9
20001 3:6
2001 4:14, 8:17, 8:20
2006 4:15, 19:18, 19:19, 64:13, 80:19, 81:3, 87:11, 87:14, 87:19
202 3:7, 31:12
2024 1:11, 8:18
2025 1:17, 92:18, 93:9
2027 93:11
21 32:3
22 45:11
24 53:18
25 77:4, 85:7, 93:9
26 45:16
27 45:15, 85:7

3

30 1:18, 40:21, 40:22, 41:8, 92:18
31 93:11
32 44:16, 45:11

3200
3:14
344
3:7
35
15:17, 16:6, 39:21, 40:2
355
3:16
37
4:12, 41:16
375
53:7, 53:12, 53:22, 54:11, 57:5, 57:12, 76:18
38
41:16

4

40
86:9
4000
3:7
42.53
89:11
43
16:6, 90:3, 92:18
44
26:15
46
26:15
48
4:13, 40:21, 41:9

5

50
62:9, 73:6
5070
3:16
54
9:1, 9:6, 9:7, 16:19, 79:11, 79:15
552
51:15
553
48:10, 51:11
554
50:12
55402
3:15
56
31:22, 61:14
571619
1:20

6

60
3:13, 77:21
600
3:5
612
3:16
62
43:12
651
8:5, 8:17, 9:12, 9:14, 14:12, 26:12, 26:14, 27:4, 27:10, 31:7, 31:22, 39:18, 57:8, 57:16, 57:17, 61:4, 61:11, 65:14, 69:5, 73:20, 76:17, 77:1, 77:21, 78:7, 79:11, 79:17, 79:19, 85:6, 86:4, 87:5
67
43:12, 57:16, 57:17
685
76:18
6th
3:13

7

70
12:2, 12:6, 12:12, 12:15, 73:20
73
4:4, 39:17, 39:21

9

9
1:18, 92:18
9,665,685
1:13
9,965,651
1:12
93
1:21