

UNITED STATE PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DATAVANT, INC.,

Petitioner,

v.

VIGILYTICS, LLC,

Patent Owner.

IPR2024-00226
Patent 9,118,641 B1

Record of Oral Hearing
Held: February 12, 2025

Before THOMAS L. GIANNETTI, BRIAN J. McNAMARA, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

JUSTIN J. OLIVER, ESQUIRE
Venable, LLP
600 Massachusetts Avenue, NW
Washington, D.C. 20001
(202) 721-5423

ON BEHALF OF THE PATENT OWNER:

NICHOLAS W. STEPHENS, ESQUIRE
W. KARL RENNER, ESQUIRE
Fish & Richardson, PC
1000 Maine Avenue, SW
Suite 1000
Washington, D.C. 20024
(202) 783-5070

The above-entitled matter came on for hearing on Wednesday, February 12, 2025, commencing at 2:00 p.m., by video conference.

P R O C E E D I N G S

- - - - -

JUDGE GIANNETTI: This is the final hearing in IPR 2024-00226 involving patent 9,118,641. Parties are Datavant, Inc., Petitioner, versus Vigilytics, LLC, Patent Owner. I am Judge Giannetti. I will be presiding at the hearing today. With me on the panel are Judges McNamara and Amundson. Let's get your appearances, starting with the Petitioner.

MR. OLIVER: Thank you, Your Honor. Justin Oliver on behalf of the Petitioner, Datavant.

JUDGE GIANNETTI: Thank you, Mr. Oliver. Anyone else on your team?

MR. OLIVER: Listening in is Nick Marcello, also at Venable, on behalf of the Petitioner.

JUDGE GIANNETTI: Okay. And you'll be making the presentation here, Mr. Oliver, I take it?

MR. OLIVER: Yes, Your Honor.

JUDGE GIANNETTI: Okay, fine. And who's appearing for the Patent Owner?

MR. RENNER: Good afternoon, Your Honors, this is Karl Renner from Fish and Richardson on behalf of Patent Owners. And I'm joined in the room today by Andy Paris, the president and CEO of Vigilytics, as well as colleagues of mine, Jeff Barclay, Indranil Sarkar, and Nick Stephens. Your Honor, Nick Stephens plans to do most of the presentation. You may hear from me again.

JUDGE GIANNETTI: All right, fine. Thank you very much, Mr. Renner. So let me go over a few details before we get started. Each side has

1 60 minutes, and each side may reserve time for either rebuttal or surrebuttal
2 as appropriate. Up to half of that 60 minutes can be reserved.

3 If there are any problems with being heard or hearing or any other
4 technical problems, please contact our IT representative who set up the call.
5 When you speak, please identify yourself if you haven't spoken for a while.
6 And please mute yourself when you're not speaking. Are you hearing an
7 echo? I'm hearing an echo.

8 MR. OLIVER: No, Your Honor.

9 JUDGE GIANNETTI: Okay, maybe that's just my connection. I
10 think --

11 JUDGE MCNAMARA: This is Judge McNamara. I'm hearing an
12 echo and a lot of static. So I just want everyone to be aware of that.

13 JUDGE GIANNETTI: Yes.

14 JUDGE MCNAMARA: So you may need to speak a little bit more
15 slowly so that we make sure that we get it all. But there is a fair amount of
16 static.

17 JUDGE GIANNETTI: All right.

18 JUDGE MCNAMARA: The best way I know of, though, to deal with
19 the muting issue, I'm sorry, with the echoing issue, is for all of us to mute
20 when we are not speaking.

21 JUDGE GIANNETTI: Okay. All right, well, let's try to do that. If
22 we have to set up the call again, we'll do that. But let's try to make it
23 through and please mute yourself when you're not speaking.

24 As you probably know, we have the complete record before us, so if
25 you need to refer to the record, please give us a page number. You will have
26 demonstratives, I take it. And the same rule applies there. We need to have

1 you, if you refer to the demonstratives, to refer to the page number. We
2 have them. But if you prefer to share your screen, you may do that also.
3 But we do have a complete set of demonstratives available to us.

4 There's no visible clock. Judge Amundson will be keeping time, and
5 we'll try to give you a warning when you get to the end of your time periods.
6 When the argument is over, please stay on the line so that the court reporter
7 can ask any questions about spellings, et cetera. The panel will probably
8 sign off at that point, but if you stay on the line, the court reporter will be
9 able to ask any questions. So that's it from us. Any questions from the
10 Petitioner or Patent Owner?

11 MR. OLIVER: No, Your Honor. None from Petitioner.

12 JUDGE GIANNETTI: Mr. Renner, from you?

13 MR. RENNER: None from the Patent Owner either, Your Honor.
14 Thank you.

15 JUDGE GIANNETTI: Okay, so let's get started then. So, Mr. Oliver,
16 do you want to reserve any time for rebuttal?

17 MR. OLIVER: Yes, Your Honor, 15 minutes, please.

18 JUDGE GIANNETTI: Okay. All right. Whenever you're ready, you
19 may proceed.

20 MR. OLIVER: Thank you, Your Honor. Good afternoon, and may it
21 please the Board. The 641 patent describes a centralized database of
22 deidentified healthcare data. The deidentification is achieved through
23 tokenization, in particular encrypting patients' personal information. Such
24 tokenization allows for searching for specific patient records. Those
25 concepts, however, have been well known in the field. In particular, Ground
26 Two's Evenhaim and Settimi references use similar tokenization methods,

1 namely hashing. And Settimi teaches a centralized deidentified database in
2 which the patient records are identified only by their tokens, just like in the
3 641 patent. Given these clear teachings, Patent Owner has put up little
4 rebuttal to Ground Two, making it the most useful ground for us to focus our
5 discussion on here today.

6 For context, in response to Ground Two, the Patent Owner argues first
7 that the references teach away from the combination. However, as we will
8 discuss, that is a narrow reading of the references, and there is no teaching
9 away. Second, Patent Owner argues that the operations would not comply
10 with HIPAA. That argument defies the fact that the references are explicitly
11 directed to complying with HIPAA. And it also contradicts the 641 patent's
12 own disclosure, which describes using similar methodologies to comply with
13 HIPAA.

14 Ultimately, Vigilytics' HIPAA argument is misdirection. It is
15 premised on a theoretical bad actor that might try and attack a system. But as
16 we'll discuss, Vigilytics' own expert acknowledges that defenses to such
17 attacks were well known. As we'll also discuss, Evenhaim provides a
18 specific defense to that type of attack.

19 Moreover, the argument misses the point. The question here is one of
20 obviousness. The attack is one about implementation options, which options
21 are neither required by the claims nor disclosed in the 641 patent. Judge
22 Giannetti, it seems like you're speaking, but I'm not hearing you.

23 JUDGE GIANNETTI: Mr. Oliver, HIPAA seems to be mentioned
24 quite a bit in the papers of both sides, and I'm not exactly sure what role
25 HIPAA plays in this case. The claims don't say anything about it. And as I

1 recall it, the Patent Owner said that this patent is not limited to HIPAA
2 applications. So what role does HIPAA play?

3 MR. OLIVER: As we'll discuss here, Your Honor, I don't think it
4 really plays much of a role, if any. All of these references are directed to
5 complying with HIPAA. There is no specific requirement in the claim to
6 comply with HIPAA other than Claim 8. And with respect to that
7 requirement, it's left up to the person of ordinary skill in the art to do
8 whatever is needed to comply with HIPAA. If that's true of the 641 patent,
9 it would be true of the prior art.

10 JUDGE GIANNETTI: For something that doesn't matter, there's an
11 awful lot in your briefing about HIPAA.

12 MR. OLIVER: Your Honor, I think it went down a little bit of a
13 rabbit hole there, I'll be honest. I agree with you. I don't think it really
14 matters. But it seemed to be a big argument raised by the Patent Owner that
15 the references wouldn't comply with HIPAA. Ultimately, I don't think that
16 matters, and I'll discuss why. But in any event, we have provided reasons
17 why we disagree with those specific arguments.

18 JUDGE GIANNETTI: Okay. Well, that's it for now. Thank you very
19 much, Mr. Oliver. I'm sure we'll be hearing more about this as we go on.

20 MR. OLIVER: I'd like to provide a little bit of context before
21 jumping into Ground Two. And I direct the panel's attention to slide 3. I
22 won't share the slides right now, as I know you have them. Just as a very
23 quick overview, and I'll come back to Ground Two. But I want to give a
24 little bit of foundation for our conversation. And that is first, that both the
25 Evenhaim and Settini references are directed to similar encryption schemes,
26 namely using hashes. Settini provides a database where all the records are

1 deidentified using their tokens. Evenhaim provides a way of saying, hey,
2 we're going to search for database records for specific patients. Put those
3 things together and you basically perform a search of a database for the
4 records that you want, which in this case are identified by tokens. That at
5 the heart of it is what the combination is all about.

6 Now, before jumping into the arguments that the Patent Owner makes
7 in rebuttal, I just want to provide a little bit of context on the 641 patent.
8 And I'll touch again very quickly on HIPAA, but I'd like to really focus on
9 the --

10 JUDGE GIANNETTI: Mr. Oliver, before you go forward, am I to
11 assume that Ground One is no longer in the case?

12 MR. OLIVER: No, Your Honor. I'll discuss Ground One as well. I'll
13 discuss it after Ground Two. The reason I'm discussing Ground Two first is
14 because many of the arguments raised by the Patent Owner in response to
15 Ground One are rendered moot. So our argument for Ground One are your
16 arguments are wrong, but they're also mooted by Settimi. So I will discuss
17 in the connection with Ground Two why the arguments against Evenhaim
18 are wrong and why Settimi renders it either way.

19 JUDGE GIANNETTI: Thank you.

20 MR. OLIVER: So it's just a useful sort of tool for our discussion.

21 JUDGE GIANNETTI: Okay, thank you.

22 MR. OLIVER: Now, looking at slide 7 again, I'll just touch on a
23 couple of top-level concepts. Slide 7, our demonstrative again, notes
24 HIPAA. HIPAA is about generally deidentifying information, making sure
25 that the records can't be determined by someone looking at them.

1 According to the 641 patent, and we could see this on the fourth bullet
2 point of slide 7 is all that's required is removing personally identifiable
3 information or otherwise transforming the information so that it cannot be
4 accessed. So how does the 641 patent propose to do that? Using
5 tokenization. That raises the next question. Well, what's tokenization? And
6 that's addressed on slide 8 of our demonstratives.

7 Tokenization is simply as stated on the top bullet point of slide 8.
8 Tokenization may include encrypting respective data that identifies an
9 individual. Meaning if the name John Smith is to be tokenized, you take
10 John Smith, you encrypt it, and the encrypted version of John Smith is the
11 token. That can be done as an example in the 641 patent with what's called a
12 hash function, which just encrypts that information.

13 JUDGE AMUNDSON: This is Judge Amundson. I had a question on
14 the concept of what a token is. And it's this, for example, is my or is a
15 Social Security number a token? Because it seems to me you can't identify
16 somebody just based on a Social Security number, you need some additional
17 information. So is a Social Security number a token?

18 MR. OLIVER: Technically speaking, yes, Your Honor. The premise
19 of these is you wanted to use something that would not be able to be traced
20 back to someone, and in theory that could be. So I guess that's a gray area. I
21 will note, however, with respect to slide 12 in the demonstratives that
22 demonstrates there was a specific claim construction for token provided, and
23 that claim construction was taken from the Patent Owner's claim
24 construction in another litigation. And that definition of a token is simply an
25 identifier associated with an individual that does not reveal the identity of

1 the individual. In that context, any ID that doesn't identify the person is
2 technically a token.

3 Now, putting that aside, all of the references we're talking about are
4 using some type of encryption so that what comes out is something perhaps
5 more private than a Social Security number. But I don't know that the claim
6 construction precludes your understanding, Your Honor.

7 JUDGE AMUNDSON: All right, then I have another issue or
8 question about claim construction. And it may not pertain to this ground,
9 but the Dick-Landi ground and what it means to make something
10 unattainable.

11 MR. OLIVER: Yeah.

12 JUDGE AMUNDSON: Is that a claim construction issue that the
13 panel needs to address?

14 MR. OLIVER: I think the argument that was raised by the Patent
15 Owner in the surreply is almost an implicit claim construction that is
16 attempting to read into the claims the idea of irreversible deidentification.
17 That claim term or that term does not appear in the claims, and thus it's not a
18 claim term. It's also not a claim construction that the Patent Owner has set
19 forth.

20 I agree with you, Your Honor, that that seems to be an argument that's
21 being made. My response to that would be to point to the record itself with
22 respect to the 641 patent and I direct the panel's attention to slide 8 of the
23 demonstratives. Excuse me, actually, one moment. Actually, slide 45 of the
24 demonstratives. The 641 patent states, and this is in the patent at column 2,
25 lines 37 to 42, tokenization may include encrypting respective data that
26 identifies each individual. If tokenization in the 641 patent is simply

1 encrypting respective data, then Landi would qualify because it is
2 encryption. There is nothing in the claims that requires it to be
3 unencryptable. In fact, when we talk about encryption, encryption usually
4 means there can be decryption. An example of encryption given in the
5 patent is hashing. Hashing is in fact one way, but it's just one example. So I
6 think to answer your question is if we look at the record of the 641 patent,
7 there's nothing that says you can't have decryptable encryption.

8 JUDGE AMUNDSON: Okay, I think I understand your position. I
9 had just one other follow up question on that and maybe you haven't been
10 able to look at this, but is there anything in the prosecution history, maybe
11 perhaps an implicit claim construction by the examiner when the examiner
12 mapped the prior art to the claim limitations? Is there anything there that
13 might help us?

14 MR. OLIVER: I'm not aware of any, Your Honor. And again,
15 because this argument of irreversible deidentification was raised in a
16 surreply and wasn't presented as a claim construction, Patent Owner has not
17 raised anything that would say what the basis is for reading in that claim
18 term, that term that does not appear in the claims. But no, I'm not aware of
19 anything in the prosecution that would suggest that that should be read into
20 the claims.

21 JUDGE AMUNDSON: All right, thank you.

22 MR. OLIVER: So with that, I'd like to just point out one last piece of
23 background before jumping into the combination, and that's on slide 11 of
24 the demonstratives. And I want to make this point because again I know it
25 probably is not maybe relevant, but because HIPAA is argued significantly

1 by the Patent Owner, I think it should be at least acknowledged how their
2 641 system works.

3 And if we look at slide 11, which is figure 3 of the patent, on the far
4 left we have the user, which is highlighted. The user might be an insurance
5 company that says hey, I want the healthcare information for this group of
6 500 people because I want to know the risk of insuring them. That user
7 sends the list of names that it wants to what's called the encryption server.
8 And as we know from the claims, particularly Claim 7, the system claim,
9 there is an encryption server that can take individual names or individual
10 identification information and create a corresponding token for each
11 individual. That's what's done at the top. That information or that is done
12 because in the middle of that figure is a deidentified data server. That's just
13 a database that has records of healthcare where instead of having name, date
14 of birth, Social Security number or whatever, we have some tokenized
15 version of it, an encrypted version of that information. So the encryption
16 server takes John Smith's name, creates a token, sends it to the database.
17 The database looks for a match.

18 Now the reason I'm sort of giving this as an example is because one
19 last point, the source entities that populate that database, which are at the
20 very bottom, could be doctor's offices, hospitals, or other healthcare
21 providers. They provide that information that gets deidentified. And I'll
22 note that the token generator, the thing that actually performs the
23 tokenization, is provided up at the encryption server at the very top. And I'll
24 refer to that as being out in the wild, meaning it's not part of the source
25 entities at the very bottom. It's not part of the doctor's office. It's something
26 existing out in the wild, separate from the doctor's office that creates tokens.

1 Why is this important? Because I think a lot of the arguments that the Patent
2 Owner makes about HIPAA is that having that ability to create a token out
3 in the wild could lead to misuse and therefore there might be problems with
4 HIPAA.

5 Putting aside whether or not that is a problem or not that it's a problem
6 in reality, it would be a problem of equal measure for the design of a 641
7 patent. And as we'll discuss, the Patent Owner's own expert, when asked
8 about this, said, and I'll direct the panel's attention to specific places,
9 particularly Exhibits 1014, pages 25 through 28. He was asked about this
10 and he said, well, you would do just general security measures to make sure
11 that that's not a problem. If that's the answer that someone would have to do
12 to comply with HIPAA for the 641, there's no reason the person of ordinary
13 skill in the art would not do the same thing for any other system that they
14 were designing making a lot of these HIPAA arguments really a bit of
15 misdirection.

16 Now, with that context, I'd like to get into the grounds. And I will
17 touch on one more HIPAA issue before I do, and that is on slide 14 of the
18 demonstratives. HIPAA specifically allows for deidentification either using
19 the expert determination method or the Safe Harbor method. And I just
20 want to note the expert determination method is, as quoted at the top of slide
21 14, about using statistical and scientific principles to deidentify information.
22 And as we can also see in the parenthetical statement, it's done so to make
23 sure the risk is small. No system is perfect. The idea here is to do the best
24 scientific job you can to try and make sure that information that's not
25 supposed to be disclosed is not disclosed. And that's what HIPAA is all
26 about.

1 So that brings us to Ground Two, and again, I'm focusing on Ground
2 Two because some of the arguments made by the Patent Owner against
3 Ground One simply are rendered moot by Ground Two, making it the easiest
4 place for us to start.

5 JUDGE MCNAMARA: Counsel, let me interrupt. This is Judge
6 McNamara. Before you start getting into that, and I understand why you
7 want to go there. But we've been thrown around a lot of terms, and I just
8 want to get a little clarification between tokenization and encryption. I can
9 assign a number, like, let's say 5-8-9-7-3 to the identity of a person, and that
10 seems like it would be a token that would be associated with an identity. I
11 can't tell the identity of that person from that number. But that's not
12 encrypted. And so I can encrypt the token so that I can't even figure out
13 what the number is later on. So I'm trying to get a distinction between
14 tokenization and encryption because we've been throwing these terms
15 around, and I see them thrown around in the patent, and I see them thrown
16 around in the arguments, and I just want to make sure I understand the
17 difference. So what do you see as the difference between tokenization and
18 encryption?

19 MR. OLIVER: Certainly, Your Honor. I would describe it as a
20 genus-species relationship. Tokenization, as you point out, and as the claim
21 construction that has been adopted by both sides point out, is simply putting
22 some information in place of the identifying information.

23 You're right, Your Honor, that tokenization in general can be just
24 assigning a code, 1-2-3-4, without performing encryption. So encryption is
25 not needed by the use of the term token in the patent or in the claims itself.
26 However, encryption is a species. It is one way to tokenize, and it is the

1 common way to tokenize, and it is actually the way all of the references
2 perform tokenization. And for that reason, we're focusing on encryption
3 because, one, that's what the references use. And two, the patent says that
4 encryption certainly is a form of tokenization. Does that answer your
5 question?

6 JUDGE MCNAMARA: Okay, I just want to make sure. Yes, I do. I
7 just want to make sure I understand what terminology everyone is using.
8 Whether or not it's one I'm comfortable with is a different question, but I do
9 understand whatever terminology everyone's using. Thank you.

10 MR. OLIVER: So we will focus on encryption just because it is a
11 qualifying species. I'll put it that way.

12 JUDGE AMUNDSON: This is Judge Amundson. I had a follow up
13 on that. And so is using a hash function on data, is that a form of
14 encryption, or is that something else?

15 MR. OLIVER: Well, the patent describes it as a form of encryption
16 and we'll go with the Patent Owner's terminology. Separately out in the field
17 some people are more precise with their terminology and might describe a
18 hash as its own unique thing. But the 641 patent certainly describes it as a
19 form of encryption.

20 JUDGE AMUNDSON: All right, thank you.

21 MR. OLIVER: That would be the common usage, yes. All right, so
22 Ground Two is combination. I'll start with slide 15 of the demonstratives.
23 First of all, Evenhaim is directed to HIPAA compliance to the extent that
24 that matters. And also as pointed out on slide 15, Evenhaim is directed to
25 performing a search of healthcare records where we are looking for records
26 related to specific individuals, as Evenhaim says, Tom, Dick, and Harry.

1 Now looking at slide 16 of the demonstratives, Evenhaim describes
2 that you want to tokenize this data or Evenhaim uses the term hash to
3 deidentify. And we can see that on the second bullet point where the
4 identifying information is replaced with a unique encryption key such as a
5 one-way hash, which is the example encryption method provided in the 641
6 patent.

7 The criticism that, or problem that Evenhaim was trying to solve is
8 Evenhaim did not like that prior methods when they created deidentified
9 databases would aggregate the data too much such as up to what we can see
10 on the third bullet point is up to the physician level, meaning you can no
11 longer see the records individually for each person. Instead all of the
12 records were sort of lumped together and assigned to one physician or
13 assigned to one zip code or otherwise made so it's lumped together in a way
14 that you couldn't see individual records. And Evenhaim said that's a
15 problem because I want to see specific records for specific patients. I don't
16 need to know which record corresponds to what patient, but I need the
17 records for these particular patients. And that's what Evenhaim is about.

18 And the way Evenhaim does that is shown on slide 17 of the
19 demonstratives. On the far left we have a user that says, I want the records
20 for Tom, Dick, and Harry. It sends the names Tom, Dick, and Harry to the
21 middle, which is the aggregator, which is the equivalent of an encryption
22 server. And as we'll discuss, that aggregator in the middle formats that
23 information and sends it on to a database for searching in whatever language
24 that database understands. That database would be the data server in this
25 situation. So that's what Evenhaim does. So what's Patent Owner's
26 criticism?

1 JUDGE GIANNETTI: Counsel, where does the matching take place
2 in this figure? Matching that's called for in the claims.

3 MR. OLIVER: Yeah. So matching takes place on the right, on the far
4 right at the data server. And as we'll discuss with the combination, the
5 proposal is to use Settimi's database in place of the existing databases. And
6 the reason for that is that Settimi provides one centralized database where
7 everything is already deidentified and identified by token. So that instead of
8 having to go in Evenhaim to five different databases and search each one of
9 them, you search one centralized repository, which is what Settimi describes.

10 JUDGE GIANNETTI: So you're not urging that there's a central
11 database in Evenhaim, are you?

12 MR. OLIVER: No, but a central database is not required by the
13 claims. A database is required by the claims. Evenhaim happens to go to
14 multiple different databases.

15 JUDGE GIANNETTI: Okay, thank you.

16 JUDGE MCNAMARA: Counsel, this is Judge McNamara. I just
17 want to make sure I understand your argument. Essentially, you're saying
18 that Evenhaim sought to get more refined information, records about specific
19 persons without identifying who those people are. Is that right?

20 MR. OLIVER: That's correct, Your Honor.

21 JUDGE MCNAMARA: Okay, thank you.

22 MR. OLIVER: Now, the issue that Patent Owner raises with respect
23 to Evenhaim we can see on slide 18, and this is why I'm dealing with
24 Ground Two first, because Settimi really remedies this. But it's a wrong
25 characterization to begin that. And that is whether or not tokenization, and
26 Patent Owner does not dispute that what Evenhaim does is tokenization,

1 what the Patent Owner disputes is where it takes place in that system. Does
2 it take place at the middle portion, the aggregator, or does it take place on
3 the far right at that data source? The Patent Owner's position is it would
4 only take place on the far right of the data source and not at the aggregator.
5 That's wrong for two reasons. One, specific disclosures in Evenhaim. Two,
6 because Settimi's database would require you to do it in advance because
7 you can't do it at Settimi. Settimi doesn't know names of people. It only
8 knows tokens.

9 So those are the important things to understand here. And I'll address
10 those after going after one other point, and that is on this idea that the
11 aggregator in Evenhaim does not perform tokenization. It does not do this
12 encryption of a name. I'll direct the panel's attention to slide 20 of the
13 demonstrators.

14 The quote at the top definitively proves that wrong. Evenhaim
15 explicitly says that there are numerous locations where an encryption of
16 individual identification, again, all tokenization is, is masking by, for
17 instance, encryption, individual identification, and what this says is that
18 encryption of individual identification can be facilitated at numerous places,
19 including at the aggregator processor side.

20 So Evenhaim specifically says you can tokenize at the aggregator,
21 which is the Patent Owner's main argument, that that would never take
22 place. Patent Owner's rationale for why that would never take place, despite
23 this clear statement of it, is that any encryption that were to take place at the
24 aggregator side in Evenhaim would only be general data transmission
25 encryption and not specific encryption of an individual. Well, that's false for
26 the reason we see here. It's also false for the two quotes we can see on the

1 bottom of slide 20, where Evenhaim makes clear that data transmission
2 encryption and the encryption of specific parts of the parameter list, being
3 the list of names, are two different and separate things. So the
4 characterization of Evenhaim alone is incorrect, and it becomes more
5 incorrect when we look at Settimi.

6 JUDGE AMUNDSON: This is Judge Amundson. I had a question
7 about that parameter list in Evenhaim, and it was my understanding that that
8 parameter list is basically a list of search terms. Maybe it has individuals'
9 names, but maybe it's just other search terms of a date range and a drug. Do
10 I have that right?

11 MR. OLIVER: It could be anything. It's anything that the person
12 wants to search for. Evenhaim does say that the parameter list can be for
13 specific people identifying them by Tom, Dick, and Harry. Whether it's by
14 names or Social Security numbers or date of birth, it's not important. But the
15 parameter list would have the identifying information.

16 JUDGE AMUNDSON: Okay, so what's the best place in Evenhaim
17 to look, in your view, where it says encrypt or hash a name or encrypt or
18 hash a Social Security number? What's the best cite for that?

19 MR. OLIVER: So first and foremost, the Patent Owner doesn't
20 dispute that what Evenhaim does is tokenized. It's only disputing where it
21 takes place. So I would direct Your Honor to three places. The one is what
22 we just talked about on the top of slide 20, where the encryption of
23 individual identification can be done on the aggregator side. And it goes on
24 in that parenthetical statement to say that encryption can be a one-way hash.
25 A hash is the specific example of encryption for tokenization described in
26 the 641 patent. So we have no dispute that this is tokenization. We have the

1 disclosure here that it can take place on the aggregator side. And then the
2 last place I would point Your Honor to is the quote on slide 26 of the
3 demonstratives. And I think that's really going to be the most illuminative as
4 to what's going on in Evenhaim.

5 Looking at slide 26 of the demonstratives, we have a large quote
6 there. I think the most important of it begins with the second highlighted
7 portion, the term converts. What happens in Evenhaim if the user sends a
8 search query? It can be for any number of things, but it can be, I want the
9 records for Tom, Dick and Harry. And as we can see in this quote here,
10 what the Evenhaim system does at the aggregator is it converts that into
11 what it calls formal language query phrases according to shared variable
12 definitions mutually accepted by the aggregator and the source entities, the
13 source entities being the databases that are being searched. So what that's
14 saying is that, okay, this aggregator takes whatever name or identifying
15 information that comes from the user and puts it in the language that the
16 database and the aggregator are speaking to each other, whatever that might
17 be.

18 And in particular, if you look at the very bottom of that quote, it might
19 be putting it in the term of a name, in the term of an ID or the like. So what
20 that's saying is the aggregator is going to take the list of names you want and
21 it's going to put it in whatever format is understood by the database. It
22 doesn't have to be a name. It might be an ID, which is basically what a
23 token is, or it might be something else.

24 Settimi's database doesn't understand names. It is a centralized
25 database where all of the records have had removed identifying information,
26 and all that's left are the tokens, which is essentially an ID. Therefore, if

1 we're talking about searching in the context of what Evenhaim does, and it
2 has to format this in a way that the database understands, the database only
3 understands tokens. And because we know that Evenhaim says you can
4 tokenize, you can do that hashing at the aggregator, all you're doing is
5 putting the query in the language the database understands. That, in a
6 nutshell, is what Ground Two is all about.

7 JUDGE AMUNDSON: Okay, all right, thank you. I think I
8 understand.

9 MR. OLIVER: I'll also note on that same point if we look at slide 23
10 of the demonstratives, because we have now linked Evenhaim to how it
11 matches up with Settimi. Settimi also tokenizes. And I'll note, as we can
12 see from the second bullet point there, the tokenization process in Settimi
13 uses what is called EPIDs, which is just a way of saying encrypted patient
14 identifiers. And those may be formed by using hashes. So a hash function is
15 used in the 641 patent it's tokenized. It's used in Evenhaim to tokenize and
16 it's used in Settimi to tokenize. And I'll note that in that cited paragraph,
17 paragraph 41 of Settimi, Settimi says you can use other methods to encrypt.
18 So it's whatever you want to do there.

19 So basically what we have is Evenhaim says you can tokenize or
20 create this hashing at the aggregator. You're going to put it in the format
21 that is understood by the database. Settimi's database understands hashes.

22 The reason that Settimi does this, we can see at the bottom bullet point
23 is Settimi wants to maintain records for specific patients. And by using this
24 tokenization or hashing process or whatever you want to call it, if you get
25 records in this centralized database from Doctor's Office 1 and Doctor's
26 Office 2 and Doctor's Office 50, because all of it was tokenized in the same

1 way, that centralized database will know that if you went to Doctor's Office
2 1 and Doctor's Office 50 and they both deidentify that using a hash and send
3 it to your centralized database, you know that those records belong to the
4 same patient. So you can identify that these records are all for one patient.
5 So you can actually now have patient by patient records and group them
6 together per patient, which is exactly what Evenhaim wants. It wants to look
7 for patient records. So that's essentially what the basis for the combination
8 is.

9 With that, I'll address with the time I have some of the arguments that
10 the Patent Owner makes about this combination. And I'll start with slide 24
11 of the demonstratives. And there are basically three arguments that I'd like
12 to address, the first of which is on slide 24.

13 Patent Owner's argument is, wait a second. Settimi is, its example
14 search is looking for characteristics. And just for a little bit of context,
15 someone searching healthcare records might be an insurance company that
16 wants to find the records of individuals, specific individuals. It might be a
17 pharmaceutical company that wants to find people who would be well-suited
18 for a clinical trial.

19 If you're searching for people for a clinical trial, you might search for
20 give me all the people of a particular age range with a particular ailment.
21 The example search in Settimi talks about looking for things like ailments.
22 The Patent Owner's argument is that there's somehow a teaching away where
23 Settimi would never be used, its database would never be searched for
24 anything other than patient characteristics, such as this person has this
25 particular disease.

1 That's wrong for at least three reasons. First and foremost, as we can
2 see from the second bullet point, Patent Owner's own expert agrees that a
3 person of ordinary skill would have understood that a database can be
4 searched for multiple types of information. It is not limited to just searching
5 for patients or just searching for characteristics. A database can be searched
6 for whatever useful information it has. And this is actually taught explicitly
7 in Settimi, as we can see from the parenthetical quote in that same bullet
8 point on slide 24 from paragraph 61, a user may codify additional terms
9 and/or create additional rules/search algorithms dynamically. What Settimi
10 is saying is you can search my database for whatever you want. As long as I
11 have the information, that's fine. You decide how you want to search it.

12 And I'll note finally, with the last bullet point of slide 24, Settimi
13 gives an example, albeit with respect to another database in its system that
14 users may search by the EPID number, meaning you can search for anything
15 you want as long as it's terminology that appears in my database. So the
16 Patent Owner's argument that no one would never search the Settimi
17 database for anything other than patient characteristics is simply not
18 supported by the record. So that's argument one that the Patent Owner
19 produces.

20 Now the next one is on slide 25, argument two that the Patent Owner
21 makes in response to the combination. Patent Owner argues that Evenhaim
22 teaches away from searching on anything but micro level data. The
23 argument is essentially this. Patent Owner's argument is that because
24 Evenhaim talks about searching the original raw data at, for instance, a
25 doctor's office, you would never, ever search for anything but the person's
26 real name in the most raw data at the source, meaning if you were going to

1 search for John Smith, you would never search for anything but John Smith
2 at the original doctor's office from the original patient file.

3 But really what Evenhaim is about is being able to identify patient
4 level records which prior systems did not permit. That is not a teaching
5 away. It is just saying I need to find the records for the person and it doesn't
6 matter what format that is, it's just that I need to know that person's
7 particular records. And I'll direct the panel's attention back to slide 26,
8 which we've already talked about, where Evenhaim explains, and this is the
9 very bottom, the bolded and italicized language, that you could search by
10 name, ID or the like, meaning that Evenhaim doesn't care whether you're
11 searching the records for the original name of the person or an ID or
12 something else. All you need to do is be able to get that person's records.
13 Evenhaim doesn't care how you search for that record, just that you get the
14 record for the right person. And therefore the idea that Evenhaim would
15 teach away from searching for anything other than the original name in the
16 original record is just not supported by this clear disclosure on slide 26.

17 Now, the third argument raised by Patent Owner, and I direct the
18 panel's attention to slide 27, and I'm raising this last because I know, I'm not
19 sure it's important to the overall argument. But the argument that the Patent
20 Owner raises is that the combination would somehow violate HIPAA. First
21 and foremost, both references, Evenhaim and Settini, are directed to
22 complying with HIPAA, which makes that argument specious at best. But
23 let me sort of try and clarify what I believe the Patent Owner's argument is
24 and why I think it doesn't make any sense.

25 The Patent Owner's argument is if the manner for creating the token,
26 let's assume for the sake of argument here it's a hash. I have the name John

1 Smith. I want to create the token and I hash that name John Smith to create
2 an equivalent token. Patent Owner's theory is, well, if you have the ability
3 out in the wild separate from the doctor's office to perform the hash function,
4 then what if you're a bad guy and you save in a table the name and the token
5 next to each other, maybe then when you see a record some other time that
6 has a hash, you could say, oh, I know that hash matches the John Smith. So
7 it's what I call the theoretical bad actor. And the argument seems to be, well,
8 that's a potential problem and therefore no one would do any of this. As I
9 noted at the very beginning, when I talked about Figure 3 of the 641 patent,
10 the token generator in the 641 patent is out in the wild. It's not at the
11 doctor's office. So to the extent that this is a concern, it would be a concern
12 for the design of the 641 patent as well.

13 And when asked about this, as I pointed to the Exhibit 1014 exhibit
14 testimony by the Patent Owner's own expert at pages 25 through 28, he was
15 asked about this. And his answer was essentially we could see on slide 27 in
16 the last quote, a POSA would understand that it would apply known security
17 techniques. So the answer for the 641 patent is you just do whatever you
18 need to do to make sure the system is secure. If that's the case, then the
19 same would be true of any of these combinations and the Patent Owner's
20 HIPAA argument simply doesn't make any sense.

21 To the extent the Board wants to entertain that argument, I'll note that
22 there are several ways to guard against it that are known in the field, and I'll
23 start at slide 29 that lists them. I won't spend a lot of time on these, but I'll
24 just make a few salient points. The first is salts. It's a way to sort of pepper
25 additional information into a token to make it so that it doesn't match up
26 anymore and sort of rebut this type of attack.

1 The only thing I want to point out that is from the site at Exhibit 1014,
2 the Patent Owner's own expert explained that the type of attack that the
3 Patent Owner is talking about, which is called a plaintext attack, has been
4 known for decades, and the defense to it has been known for decades, one of
5 which is a salt. So this is something that would just be the manner of
6 implementation, and it is not something that is required or addressed by the
7 claims or the specification making a little bit of misdirection.

8 Other ways to address it are additional levels of encryption. That's
9 discussed in slides 30 and 31 of our demonstratives. I won't spend much
10 time on that other than to say that in the original declaration from the
11 Petitioner's expert, the expert explains, look, if you're worried about these
12 types of things, you just doubly encrypt or triply encrypt or you encrypt
13 again so that the token that you release out in the wild is not going to match
14 whoever that bad actor, whatever token they have. It's just an easy way to
15 do away with it.

16 And the last one I'll talk about, I will spend a minute on, and that's the
17 trusted broker agent. I direct the panel's attention to slide 32. Evenhaim
18 already accounts for this issue. Evenhaim says, look, the aggregator can be
19 the place where this encryption hashing takes place. But as discussed there
20 in column 12, it's cited and as explained by the quotes from Patent Owner's
21 own expert, what Evenhaim explains is that, look, if you don't really trust the
22 aggregator, you simply have what's called a trusted third party, such as an
23 escrow agent, hold the key, meaning yes, the aggregator position is
24 performing this encryption, but if you don't trust them, have an escrow agent
25 hold this and therefore the aggregator really doesn't technically have the

1 ability to do what you're worried about. Someone else actually holds the key
2 and that keeps the system safe.

3 So these would rebut the problems that the Patent Owner seems to
4 think are problems. But again, they're things that are not required by the
5 claims, they're not required by the specification, and therefore we don't think
6 there are proper rebuttals to begin with.

7 So with that, those are the rebuttals to Ground Two. And this is why
8 we believe that Ground Two renders all of the claims unpatentable.

9 JUDGE AMUNDSON: This is Judge Amundson. I think you got
10 about five minutes left in your initially requested 45.

11 MR. OLIVER: Sure. With the few minutes I have left, I would like
12 to turn to Ground One to highlight one salient point. I will leave given the
13 time the Dick-Landi combinations for the briefing.

14 With respect to Ground One, I would just direct the panel's attention
15 to slide 35. Again, most of the arguments and points I've raised with respect
16 to the teachings of Evenhaim apply equally to Ground Two and Ground
17 One. Just the explanation that the hand-and-glove fit between Settimi and
18 Evenhaim just makes it a little bit easier to explain.

19 But I do want to highlight one point in the context of the Ground One
20 alone, and that is going back to just our context of what is Patent Owner's
21 argument. Patent Owner's argument is that the system in Evenhaim would
22 only at the aggregator use what's called data transmission encryption,
23 meaning anytime you're going to send a message over the Internet or some
24 other method, you would want to encrypt the whole message. That message
25 then gets decrypt at the recipient side so they can read it. Patent Owner's
26 argument is that anything that Evenhaim is talking about the aggregator can

1 only be general data transmission. Everything will be decoded at the data
2 source, including the name John Smith. And therefore you would only
3 search the name John Smith.

4 Patent Owner's own expert, when the portions of Evenhaim were
5 pointed out to him, that explained that data transmission encryption and
6 encryption of the parameter list are two different things, he explained it in a
7 way that really rebuts the Patent Owner's argument. And that's set forth on
8 slide 35. Essentially when he was pointed to the portions of Evenhaim that
9 say here's data transmission encryption, here's the heightened encryption that
10 we use for fields in the parameter list. A field in the parameter list, maybe
11 it's name, maybe it's date of birth and name or something else. That
12 heightened encryption, he said, is different than data transmission
13 encryption. And what he called it, the Patent Owner in its slides referred to
14 this as a new argument by Petitioner. This is not Petitioner's words. This is
15 the Patent Owner's own expert's words. He called it in his testimony super
16 encryption. And his explanation of super encryption was that that super
17 encryption of a field in the parameter list, maybe its name and date of birth,
18 would not be decrypted at the receipt recipient side. And you can see that in
19 the testimony that's cited there from 1014 around pages 74 through 79.

20 But what he explained is that is never decrypted. That is kept
21 encrypted. Patent Owner's argument in rebuttal to Evenhaim is that you
22 would always perform decryption of the parameter list at the source side and
23 always then search using the names. Patent Owner's expert says no. It
24 seems like what they're saying here is never going to be decrypted at the
25 source side. If the Patent Owner's own expert blows up their rebuttal to
26 Evenhaim, then Ground One is also proper. And I do not want to leave the

1 impression that we are giving up on Ground One. I simply put them in this
2 order for ease of explanation.

3 With that, absent any questions, I'd like to reserve the rest of my time
4 for rebuttal.

5 JUDGE GIANNETTI: I think you, check with Judge Amundson, but
6 I think you have your full 15 minutes for rebuttal, is that correct?

7 JUDGE AMUNDSON: This is Judge Amundson. Yes, I think you
8 have actually 16 minutes.

9 JUDGE GIANNETTI: Sixteen minutes. Okay. All right. So you
10 have 16 minutes, Mr. Oliver. Thank you very much. I don't hear any
11 questions from the panel, so let's turn now to the Patent Owner. You may
12 proceed when you're ready, Counsel.

13 MR. STEPHENS: Thank you, Your Honors. And may it please the
14 Board, Nicholas Stephens on behalf of Patent Owner Vigilitics. Your
15 Honors, while I'd be happy to take any questions on Ground One based on
16 Evenhaim alone, I do plan as with the Petitioner to begin with Ground Two
17 in view of their more recent focus on this ground.

18 JUDGE AMUNDSON: This is Judge Amundson. Before you get
19 into it, could I ask if you want to reserve any time for surrebuttal?

20 MR. STEPHENS: Thank you, Your Honor, we would like to reserve
21 15 minutes, please.

22 JUDGE AMUNDSON: Okay. Very well. Okay. Sorry to interrupt.
23 Go ahead.

24 MR. STEPHENS: As to the Evenhaim-Settimi combination --

25 JUDGE GIANNETTI: Let me also ask a preliminary question here,
26 Mr. Stephens. Do we have a claim construction dispute over the term

1 tokenization? Is Patent Owner on board with the definition of tokenization
2 that we saw on slide 8?

3 MR. STEPHENS: Your Honor, we've not disputed the construction
4 of token as it is in isolation presented in the petition, but I think we can't just
5 view the terms by themselves. So there are certain limitations when we get
6 down to the Dick-Landi ground, for example. Limitations in each of the
7 independent claims that require the produced healthcare information to be
8 absent personally identifying information.

9 JUDGE GIANNETTI: I don't think that was quite my question. I'm
10 just asking you simply whether you go along with that definition or
11 construction, if you will, of tokenization.

12 MR. STEPHENS: We've not disputed it. The argument that we've
13 raised in the briefs, we can distinguish the references on other bases.

14 JUDGE GIANNETTI: Okay. All right, thank you very much. You
15 can proceed.

16 MR. STEPHENS: As to the Evenhaim-Settimi combination, Datavant
17 contends, and indeed must show to satisfy the claims, that it would be
18 obvious to modify Evenhaim to search patients' deidentified healthcare data
19 rather than the original non-deidentified data at the data source entities. To
20 this end, the petition proposes integration of Settimi's centralized warehouse
21 of deidentified records such that in the combination, Evenhaim's data
22 aggregator would query the warehouse of deidentified data. This proposed
23 integration, however, suffers from two related but distinct legal problems.

24 First, Evenhaim teaches away from the very technique that Datavant
25 is proposing to apply in the combination, and that is searching on
26 deidentified data.

1 JUDGE GIANNETTI: Would you point to me specifically where that
2 is? Teaching away is a term that's thrown around a lot, but specifically, you
3 have to show that the disclosure is pointing you in a different direction.
4 Where exactly is that? Can you point specifically where in the disclosure of
5 the patent that this teaching away takes place?

6 MR. STEPHENS: Yes, Your Honor, I'd be happy to. In fact, there's a
7 number of places. I'll point you to a number of them, to several of them, but
8 we see this throughout --

9 JUDGE GIANNETTI: Give us your best one. Give us your best one
10 for now. Okay. And we can look through the other ones later. Give us your
11 best teaching away argument.

12 MR. STEPHENS: Yes. If Your Honors would look at column 4,
13 lines 42 to 45.

14 JUDGE GIANNETTI: You have that on the slide, or should I just go
15 back to the original document?

16 MR. STEPHENS: If you're able to pull open the original document, I
17 think that would be most helpful.

18 JUDGE GIANNETTI: Okay, so we're looking in Evenhaim, right?

19 MR. STEPHENS: We're looking at Evenhaim, in column 4, lines 42
20 to 45.

21 JUDGE GIANNETTI: Column 4, 42 to 45. Okay, I've got it.

22 MR. STEPHENS: Yes. And here, Your Honors, Evenhaim describes
23 that HIPAA provides substantial limitation on personal health information,
24 and existing deidentification methods may render the information useless for
25 the purpose of measuring the impact of health programs. So in context,
26 what's being discussed here is that traditionally there are classic models

1 described in Evenhaim in which data warehouses would house deidentified
2 data. This deidentified data is deidentified according to methodologies that
3 comply with HIPAA. There's what's called the Safe Harbor method of
4 deidentification in HIPAA, and there's also a statistical method of
5 determination of deidentification.

6 But what Evenhaim is saying here is that to query on the deidentified
7 data does not allow you to access the most granular aspects of the patient's
8 file. And that's what Evenhaim was truly concerned with.

9 JUDGE GIANNETTI: But wait a minute, aren't you reading a lot into
10 that one sentence? Well, the way I read it, they're just saying that HIPAA
11 provides a substantial limitation, so it has to be deidentified, and so the
12 information may be useless. But that doesn't say anything about searching
13 that data, that there might be other ways of searching it. I think you're
14 reading a lot into that sentence, Counsel.

15 MR. STEPHENS: I think we have to contextualize not just the
16 statement in isolation, but also looking across the disclosure. So, for
17 example, at column 3, line 49. Evenhaim expresses its concern with the
18 classic models in which you have deidentified data. It says a portion of the
19 original data set is lost and no longer available for analysis. So he's
20 lamenting the fact that when you deidentify data, a portion of the data is
21 gone. It's no longer available for analysis. That's why HIPAA deidentified
22 data, as described at column 4, is not suitable for the purposes that Evenhaim
23 was seeking to achieve.

24 JUDGE AMUNDSON: This is Judge Amundson. Let me tell you my
25 understanding of what I think Evenhaim is directed to, and you can tell me
26 where you think I'm wrong, if you think I'm wrong. But as I understand

1 Evenhaim, they were trying to get at a specific issue where if you wanted to
2 get healthcare information for specific patients, you couldn't follow exactly
3 HIPAA rules. And so they get around it one way or another. But it seems to
4 me they're not criticizing searching for deidentified data for other purposes.
5 For example, you've had a new advertising campaign and to see if your sales
6 went up. Am I misunderstanding Evenhaim?

7 MR. STEPHENS: Well, the reason that Evenhaim distributes its
8 query from the aggregator to the original data source entities, one of the
9 problems with the classic models where you have deidentified data, you
10 can't search by names. So you cannot, in those models it's a longitudinal
11 search. You search for attributes of the patient, you look at whatever data
12 may remain in the deidentified records, what medications they're on,
13 demographic data. But you cannot search for specific individuals.

14 And that's the problem that Evenhaim really saw with these
15 deidentified databases, is that when you deidentify, you're no longer able to
16 search for known individuals. He gets around this. His solution is to have
17 the aggregator issue the queries to the healthcare providers, the data source
18 entities that maintain the original patient data files. And that's the only way
19 that Evenhaim could search on the original names, because the data is not
20 deidentified. You have the raw original data, the data source entities.

21 JUDGE AMUNDSON: All right, thank you.

22 JUDGE GIANNETTI: You can proceed, Counsel.

23 MR. STEPHENS: Thank you, Your Honor. I'd like to, just to further
24 contextualize this. We really see the same concern expressed throughout
25 Evenhaim in its background discussion, the detailed description, its
26 summary of the invention, when it gets to the end of the disclosure and is

1 contrasting the solution in Evenhaim with the prior approaches. Multiple
2 times he laments the fact that when you're searching or analyzing on
3 deidentified data, you're not able to search for individuals. You cannot
4 perform the high-resolution analysis that Evenhaim sought to do.

5 So, for example, at column 4, this is again the same paragraph we
6 were looking at earlier up above, he explains that there's a challenge in
7 measuring the impact of a consumer health program that becomes significant
8 when the health program sponsor does not have the full – full -- healthcare
9 information.

10 JUDGE GIANNETTI: What's the line number again, Counsel?

11 MR. STEPHENS: Column 4, lines 34 to 39.

12 JUDGE GIANNETTI: Thirty to 39?

13 MR. STEPHENS: Thirty-four to 39.

14 JUDGE GIANNETTI: Okay, thanks.

15 MR. STEPHENS: And then if we continue onto the top of column 5,
16 you'll see that Evenhaim recognizes a long-felt need in the art for a protocol
17 that will allow higher resolution query and manipulation of privacy sensitive
18 data. So he acknowledges there were many approaches in the past to
19 searching deidentified data, not for specific individuals, but for this broad,
20 kind of longitudinal based searching. And that wasn't satisfactory to
21 Evenhaim because it doesn't allow you to perform the analysis on specific
22 individuals.

23 At column 16, I'd also direct your attention to line 63. Evenhaim
24 again expresses his concern. Column 16, line 63, one cannot query or
25 analyze parameters that are no longer in the lower resolution data set. At
26 column 7, line 46, we see that Evenhaim again critiques deidentification

1 practices that preclude external researchers from benefiting from the
2 richness of the source entity data.

3 So when we look earlier at the sentence where he critiques HIPAA-
4 compliant deidentified data in column 4, this is really in the context of all
5 these disclosures that tell us that searching under deidentified data using the
6 classic models, that's not what Evenhaim was trying to achieve. He wanted
7 to go beyond that to provide a different type of analysis than you could get
8 from the deidentified data.

9 And yet, what do we see in the combination that's been proposed by
10 Petitioner with Settimi? They're proposing to bring in a database that's just
11 like the classic models described in Evenhaim. Evenhaim is saying, "Don't
12 do that. It doesn't allow us to access the high-resolution data." And yet, in
13 this combination, they're bringing in a database that's populated with
14 HIPAA-deidentified data.

15 So in our view, we recognize, Your Honor, Judge Giannetti, you
16 mentioned earlier that teaching away, it's often alleged, many times the
17 references don't bear it out. The case law Federal Circuit is distinguished
18 between teaching away and general preferences between alternatives. We
19 don't think that this is a case where this is merely a general preference.
20 Evenhaim's characterization of deidentified data throughout its disclosure,
21 again, useless, strongly discredits the approach called for in the combination.

22 If Your Honors return to slide 16 of our demonstratives. When we
23 argued this in the Patent Owner's response, the reply that we got from the
24 Petitioner was that similar to what counsel on the other side has just argued
25 that there is just a general preference, is their view in Evenhaim. And they
26 cited to disclosure that Evenhaim would provide an option for searching on

1 identity-free microdata. But it turned out this is not true. If you look below,
2 beneath the citations, don't just take the assertion as it's made in the reply.
3 Look at what's actually cited in Evenhaim.

4 When he refers to identity-free microdata, this is data that's already
5 been searched by the data source entities, returned to the data aggregator.
6 When that data is returned, the data source entities, they deidentify the data,
7 but only after performing the search and the analysis that yields identity-free
8 microdata. So there is no option disclosed in Evenhaim for searching
9 identity-free microdata. It's not just in every embodiment. But although
10 that's true, he always searches on the original data at the data source entities.
11 And then the data aggregator receives the identity-free microdata, aggregates
12 it, and prepares an appropriate report for the user.

13 Now, as I noted earlier, there are two problems with the combination.
14 Even if we don't get to the point of teaching away -- which we, again,
15 believe that's what Evenhaim provides -- Datavant has failed to carry its
16 burden of demonstrating a sufficient motivation to implement the
17 combination with deidentified data searching. And this failure is apparent
18 when comparing the evidence that Datavant relies on to support the
19 combination with Evenhaim's own statements to the contrary.

20 The only evidence the petition cites in support of combining
21 Evenhaim and Settimi is the testimony of Petitioner's declarant, Dr. Clark.
22 So you can look at Exhibit 1003, paragraphs 134 to 138. This is where Dr.
23 Clark describes his overview of the proposed Evenhaim- Settimi
24 combination. But what do we see when we turn to that testimony? We see
25 writing that largely mirrors the petition without corroboration. But, perhaps
26 most strikingly, we see that Dr. Clark fails even to acknowledge that

1 Evenhaim's repeated concerns with searching deidentified data, let alone
2 acknowledge that the combination he proposes is directly at odds with those
3 expressed concerns.

4 JUDGE GIANNETTI: Counsel, let me make sure I understand your
5 argument. I thought your argument was because of this teaching away, you
6 wouldn't make the combination. Are you now arguing that a person of
7 ordinary skill in the art couldn't make the combination? That there's some
8 technological barrier to doing it?

9 MR. STEPHENS: Your Honor, we do agree that there's a teaching
10 away here, but the Court has told us that even if the prior art is not found to
11 teach away, its statements regarding preferences are relevant to a finding
12 whether there'd be a motivation to combine. And so, what we're just saying
13 here is we don't even need to reach teaching away, even though we believe it
14 exists, to find that Datavant has not carried its burden to show that there's
15 been a motivation to combine these references. And what particularly --

16 JUDGE GIANNETTI: Well, I have trouble separating those two
17 arguments. If there's a teaching away, isn't that in essence, a lack of
18 motivation? I mean, a person wouldn't have been motivated because they
19 would have been steered in the other direction. What's the difference
20 between those two arguments?

21 MR. STEPHENS: Well, I think we're not arguing that there's
22 necessarily an incompatibility here in which -- the issue is not whether
23 POSITA could combine the references, but as Your Honors know, it's
24 whether POSITA would have. And that's what we don't think the evidence
25 supports. When you look at the analysis that's been given by Petitioner and
26 the evidence that they've cited through their testimony of Dr. Clark, he says

1 that you combine these references. He says that a person of skill in the art
2 would do that. But he doesn't even acknowledge or recognize that
3 Evenhaim has many statements strongly to the contrary -- says don't search
4 deidentified data. So how are we supposed to weigh that evidence?

5 JUDGE GIANNETTI: Well, let me put it another way. If we were to
6 decide that there is not sufficient evidence of teaching away here, does that
7 basically resolve that issue that -- doesn't that say that there's no motivation
8 to combine?

9 MR. STEPHENS: No, Your Honors, I don't think so. Our surreply
10 and in Patent Owner's response, we referred to a decision in *Polaris v. Arctic*
11 *Cat.* That's 882-F-3rd-1056, a decision from 2018. And it's there that the
12 Federal Circuit explained that even if the prior art is not found to teach
13 away, its statements regarding preferences are still relevant to a finding
14 whether a skilled artisan would be motivated to combine the preferences. So
15 you don't need to get to teaching away to find that the Petitioner has not
16 demonstrated a motivation to combine the references.

17 JUDGE GIANNETTI: All right, thank you.

18 MR. STEPHENS: Finally, and before moving along, I'd like to
19 address one last point with respect to the alleged obviousness of searching
20 deidentified data in this combination. Specifically, in its reply brief,
21 Datavant attempts to argue that there might be some form of data available
22 in the combination that would be sufficiently robust so as not to offend
23 Evenhaim and yet still deidentified as required by the claims. But that data
24 does not exist. If we look at Settimi, paragraphs 27 and 39, this is where
25 Settimi describes the type of data that's available in its database, the database
26 that would be integrated in this combination. In these paragraphs, Settimi

1 confirms that its data is deidentified in accordance with HIPAA. So we're
2 looking at data that's been released from the healthcare providers,
3 deidentified in accordance with HIPAA, stored in the centralized database
4 that's used in the combination. But, recall, we just looked at Evenhaim at
5 column 4. This is the exact same data that Evenhaim said was useless.

6 JUDGE GIANNETTI: Do we have to accept -- if the combination is
7 with Settimi -- I think they're relying on Settimi, if I'm not mistaken, for the
8 presence of this data warehouse and also for the presence of tokenization.
9 So why do we have to accept the fact that this is deidentified data? Why
10 couldn't we -- what's the difference? Data is data, right?

11 MR. STEPHENS: This is a very critical point, Your Honor. I'm glad
12 you brought it up. Thank you. First, I would note that, go back to the
13 petition and look at how the combination is described. I believe that's pages
14 37 to 39. They make a --

15 JUDGE GIANNETTI: Petition page 37?

16 MR. STEPHENS: Yes, Your Honor. I'm pulling it up myself as well.

17 JUDGE GIANNETTI: There. Yes. It's a claim chart.

18 MR. STEPHENS: Thirty-six, Your Honors. I'll actually back up to
19 34, at the start of the overview of Evenhaim --

20 (Simultaneous speaking.)

21 JUDGE GIANNETTI: Okay. Yes.

22 MR. STEPHENS: The bottom three lines, you'll see, "The central
23 repository allows the patient data to be queried for e.g. research, while
24 keeping the centralized records HIPAA-compliant."

25 Now, this is really important. In Settimi, as in any of these references
26 that we're talking about, they all sought to comply with HIPAA. That's the

1 name of the game in this field. You have to comply with HIPAA. So in the
2 centralized database that's disclosed in Settimi, it's collecting data from what
3 Settimi refers to as patient care providers, the PCPs. Thus, the PCPs hold
4 the original patient data. But under HIPAA, the HIPAA privacy rule
5 precludes them from releasing that data without the authorization of the
6 patient unless it's been deidentified. So it has to be deidentified in order for
7 it to be released to any other entity, including the centralized data
8 warehouse, to comply with HIPAA. And I don't think that's a point that's
9 been disputed by either party.

10 JUDGE GIANNETTI: Well, the role of HIPAA is something that I
11 questioned earlier, and I believe the Patent Owner minimized the role of
12 HIPAA. And as I read your papers, you say that your patent is not limited to
13 HIPAA applications. So why the focus on HIPAA here? Why is that so
14 important?

15 MR. STEPHENS: So in our view, so characterizations of the patent
16 don't address the issue of whether there's a proper and sufficient motivation
17 to combine these references. If we look at how the combinations were
18 framed in the petition, and looking at the purposes and the goals of the
19 references themselves, they're all to comply with HIPAA. I believe
20 Petitioner's counsel just noted the same. So when we look at the motivations
21 to combine, when you bring these references together, whether they comply
22 with HIPAA speaks to whether a person of skill in the art would or would
23 not have a motivation to bring in, for example, a database like Settimi's to
24 operate in a system like Evenhaim's.

25 JUDGE GIANNETTI: Counsel, don't you think your argument is
26 really based on separately attacking the references? I mean, you say, "Well,

1 Settimi, they've got this centralized database, and they do this tokenization,
2 maybe, but the records are the wrong kind of records." And then, in the case
3 of Evenhaim, where it's the right kind of records, you say, "Well, that doesn't
4 have tokenization, and it doesn't have a centralized database." Aren't you
5 really avoiding the combination that they put forth? And then tell me why
6 the combination wouldn't meet the claims.

7 I also noticed a lack of discussion of claim language in both parties'
8 presentations. It seems that the emphasis is on the disclosures and the
9 embodiments rather than on the claim language. So maybe you could
10 address the combination that they put forth and tell me why that doesn't meet
11 the claim.

12 MR. STEPHENS: Sure, Your Honors. And we'll take the Evenhaim-
13 Settimi combination.

14 JUDGE GIANNETTI: Yes.

15 MR. STEPHENS: We proposed to bring, as we know, the central
16 warehouse from Settimi, use it with the data aggregator in Evenhaim so that
17 that data aggregator would query the database, that central database, rather
18 than the data source entities.

19 JUDGE GIANNETTI: A database of not necessarily deidentified
20 patient records. But I don't know what you would term them, raw data,
21 whatever you want to call it. The type of data that's being accessed in
22 Evenhaim.

23 MR. STEPHENS: No, Your Honors, that's not what's been proposed
24 in the petition. Thirty-four to 36, you'll see that as they've described the
25 combination, it is "The central warehouse does not have that original raw
26 data." You're not simply merging the raw data from the data source entities

1 as described in Evenhaim. We have a central warehouse of deidentified
2 data, and that's the only way under HIPAA in which that data could be
3 combined because, again, the restrictions on the release of data. If you're
4 going to release it all to a third party, it has to be deidentified.

5 JUDGE GIANNETTI: Well, Settimi's database could contain raw
6 data identified by an EPID, couldn't it? What is it about that database that
7 prevents it from doing that?

8 MR. STEPHENS: It could not, Your Honor. It would not have
9 access to the original data. It's the PCPs and Settimi.

10 JUDGE GIANNETTI: Because of HIPAA.

11 MR. STEPHENS: Because of HIPAA. That's correct.

12 JUDGE GIANNETTI: Well, HIPAA compliance. I'm still struggling
13 with the role of HIPAA compliance in this whole case. When you say that
14 your patent is limited to HIPAA, and I don't see that in the claims. So why
15 should I give that so much weight?

16 MR. STEPHENS: Well, it's deceptively complex, but I would say
17 HIPAA is in the background.

18 JUDGE GIANNETTI: Help me out there, help me out.

19 MR. STEPHENS: HIPAA's in the background of all of these
20 references. So we're looking at the structure, the architectures of the system
21 in Evenhaim, in Settimi or even in this combination. We're thinking about,
22 is it HIPAA-compliant? That's why, starting with Evenhaim for example,
23 why do they issue the queries to the data source entities to access the
24 original data? Well, it's because only the data source entities, those are your
25 healthcare providers, the doctor, that hold the original patient files. They're
26 the only ones that have the rights under HIPAA to that original data.

1 If you centralize it as they're proposing to do in Settimi, it has to be
2 deidentified. But in so deidentifying we lose some of the granularity of the
3 data that Evenhaim was concerned about.

4 JUDGE GIANNETTI: So I'm going to read you something from your
5 Patent Owner response. You say, the inventive technology is not limited to
6 systems and methods that operate within the constraints of HIPAA. You
7 agree with that, right?

8 MR. STEPHENS: As written, Claim 1 does not have the limitation
9 that requires HIPAA.

10 JUDGE GIANNETTI: And you say that your inventive technology
11 goes beyond and it's not limited to HIPAA constraints. So why are you
12 giving me a HIPAA argument?

13 MR. STEPHENS: It's the petition, in our view, that has set up
14 HIPAA as a central focus of this case.

15 JUDGE GIANNETTI: I see.

16 MR. STEPHENS: Its descriptions of the priority of the combinations
17 are all about HIPAA. The motivations to combine are to comply with
18 HIPAA. They say, Dr. Clark says, the Petitioner says, you would issue
19 queries in a HIPAA-compliant manner. The centralized warehouse in this
20 combination, they acknowledge in the petition, has to have deidentified
21 records that are maintained in compliance with HIPAA. So it goes to
22 whether this combination is obvious and whether this combination can be
23 implemented in a way that reads on the claims while still respecting the
24 constraints that are present.

25 JUDGE GIANNETTI: The claims read on that. It doesn't read on
26 claims. Claims read on things. You don't read things onto claims. That's

1 just a terminology problem with your argument. All right, well, I guess I'm
2 still somewhat surprised with the emphasis here on HIPAA when you say
3 that your technology is not limited to HIPAA. But at least I see your
4 position. Thank you.

5 MR. STEPHENS: And Your Honor, I just want to be clear. We look
6 at dependent Claims, 2, 8 and 15.

7 JUDGE GIANNETTI: Yes.

8 MR. STEPHENS: These do require that the healthcare information
9 that's produced be in conformity.

10 JUDGE GIANNETTI: I don't see much mention of those in your
11 brief. I think your brief's pretty much limit the arguments to Claim 7. Is that
12 right? Did you discuss those claims in your briefing?

13 MR. STEPHENS: In the HIPAA violations that we noted in our
14 surreply, we believe that those HIPAA violations are relevant to motivations
15 to combine that are applicable to all claims, but also pointed out that it's not
16 just relevant to motivation as to these dependent claims, but also shows that
17 it wouldn't meet these dependant claims if it's not in conformity with
18 HIPAA.

19 JUDGE GIANNETTI: Okay. Thank you. You can proceed with
20 your argument.

21 MR. STEPHENS: Your Honor, may I ask how much time we have
22 available on our direct?

23 JUDGE AMUNDSON: Yes, this is Judge Amundson. Let's see,
24 you're almost at 30 minutes in, not quite at 30 minutes in. So you've got 16
25 minutes left in your initial 45.

1 MR. STEPHENS: I'd next like to turn to slide 53, please. And here
2 I'll first address how Dick and Landi failed to meet the requirement in the
3 independent claims for producing healthcare information that's absent
4 personally identifying information, PII. Petitioner in the panel --

5 JUDGE MCNAMARA: I'm sorry, Counsel. This is Judge
6 McNamara. Did the Petitioner discuss the Landi references in his argument?
7 I don't think he did. So I don't think it's appropriate to be responding to
8 opposing them when arguments that weren't discussed during the hearing.

9 MR. STEPHENS: I understand this is our direct argument, and so we
10 are not limited to the scope of the patent.

11 JUDGE MCNAMARA: It's an opposition. It's an opposition,
12 Counsel. You're opposing the arguments that were made in the hearing.

13 MR. STEPHENS: I'm happy to continue on Evenhaim and Settimi.

14 JUDGE MCNAMARA: Do you have more to say about Evenhaim
15 and Settimi?

16 MR. STEPHENS: We do, Your Honors. There are additional reasons
17 that the combination fails. The combination fails to disclose or render
18 obvious an encryption server that produces a token for each individual
19 identified in any request. So in the claims, the tokens produced by the
20 encryption server are used for searching as they are matched against
21 corresponding tokens associated with deidentified healthcare data.

22 Now, to understand why, recall that the petition relies on Settimi's
23 encoded patient identifiers, or EPIDs, as the claimed tokens in the
24 combination. EPIDs are associated with deidentified data records released
25 from each healthcare provider to the centralized warehouse. And yet,
26 Settimi's system does not use the EPIDs to search for known individuals'

1 data records in the central warehouse. And importantly nor could they be
2 used for this purpose. This is because Settimi's central database is
3 specifically designed for longitudinal searching by clinical or demographic
4 characteristics. For example, to identify a qualifying cohort of patients for a
5 clinical trial. Once the deidentified records for qualifying patients are
6 identified from the search, the EPID can then be decrypted by the original
7 healthcare provider to re-identify the patient.

8 On slide 35, we note that there's no ability for third parties to search
9 for known patients using the EPID because only the patient care provider
10 possesses the patient identifier and the password that are necessary to
11 generate an EPID for a particular patient.

12 So in the combination, just stepping back, what they propose is that
13 Evenhaim's data aggregator would accept a request from the data consumer
14 entity. So you have a request that names a list of individuals and then
15 they're going to somehow, they say, convert that list of names into tokens
16 that could be used to search the deidentified warehouse in Settimi. And they
17 need the tokens because that central warehouse is deidentified, the names are
18 no longer available. Much of the PII has been stripped from the records in
19 the central warehouse.

20 But they say that this can be done using Settimi's EPIDs. And yet
21 there's no explanation in the record as to how that would even be possible,
22 because what Settimi tells us is that the EPID is generated using a patient
23 identifier and a password that's held in confidence by the patient care
24 provider, the original healthcare sites. And that's important because if you
25 have the password, if that password is released, any other party who obtains
26 the EPID can use the password to decrypt it and re-identify the patient. But

1 somehow in this combination, they're saying that this EPID could be
2 generated at the data aggregator to produce a token that could be used for
3 searching. And that's just not feasible with the EPIDs that are described in
4 Settimi. And again, they are relying on Settimi's EPIDs for searching the
5 centralized database. And they're asking a data aggregator that's an entity
6 that's different from the healthcare providers who would not have the
7 password, who would not have the patient identifier to somehow create these
8 patient identifiers, the EPIDs.

9 JUDGE AMUNDSON: This is Judge Amundson. I asked a question
10 of Mr. Oliver relating to claim construction and it concerns the unattainable
11 issue. And I thought maybe you were going to get there when you went to
12 your slide 53. And so I understand Patent Owner's position on the
13 unattainable term is that something has to be irreversibly deidentified. Do I
14 have that correct?

15 MR. STEPHENS: Yes, Your Honor. We believe reversible
16 deidentification would meet the claim limitation for being unattainable.

17 JUDGE AMUNDSON: Okay, now here's my follow up question. If I
18 have a name and I apply a hash function to the name, does that make it
19 irreversible? Does that make the name irreversibly deidentified?

20 MR. STEPHENS: That would be irreversibly deidentified, Your
21 Honor.

22 JUDGE AMUNDSON: Well, okay, now I have a further follow up
23 question. I understand that there are some hash functions that, over time,
24 people have been able to crack. For example, I think it's MD5 is one of
25 them. So if I applied an MD5 hash function to a name, would that be
26 making it irreversibly deidentified?

1 MR. STEPHENS: Well, again, I think we look at this and it's an
2 interesting hypothetical. It's not obviously been briefed in the record. But
3 irreversible deidentification and hash functions, the suitable hash functions,
4 would be known to one of skill in the art, and it's actually defined by Health
5 and Human Services under HIPAA. So you would use an appropriate
6 function, and whether it might be theoretically possible for that hash to be
7 correct, as long as it's a hash function that would be suitably used in this art,
8 the identities would be unattainable in that instance.

9 JUDGE AMUNDSON: Well, okay, but I think the panel, when we're
10 considering a claim construction issue, we're going to have to first turn to the
11 intrinsic evidence and not go to that government document. But okay, I
12 think I understand your position. Thank you.

13 MR. STEPHENS: For our purposes, Your Honors, I think we can
14 accept that a hash function would yield an irreversibly deidentified token.
15 That's what's described in the specification. But importantly, that's not what
16 Settimi discloses, or Landi, for that matter. So for Settimi, Mr. Oliver
17 addressed in his direct presentation, he said that there was a hash function
18 that's used in Settimi to generate the EPIDs. If we actually look at what's
19 disclosed there, and this is an argument, by the way, that's not in their briefs.
20 It appears in their demonstratives, but I am responding to this somewhat in
21 real time.

22 But what Settimi tells us is that there's a hash that can be applied to
23 the password string that the patient care provider uses as part of the
24 encryption algorithm. However, the patient identifier itself is not hashed in
25 that embodiment. So there's no suggestion in Settimi that you would
26 actually perform hashing to get to irreversible deidentification of the patient

1 identifier. What's hashed is the password string. The result of that hash is
2 appended to the PID. So in that instance, the token in Settimi, the identity of
3 the individual is not unattainable. It's, in fact, the sentence about hashing
4 follows the sentence about symmetric encryption and decryption, which tells
5 us what Settimi was trying to achieve was to allow the EPID to be decrypted
6 to allow the patient care provider to re-identify the patient.

7 JUDGE AMUNDSON: This is Judge Amundson. Judge Giannetti, I
8 think you're saying something, but you're on mute.

9 JUDGE GIANNETTI: My question is simply where is this issue
10 raised in the claims? I think we heard from the Petitioner that this may be
11 something that's not claimed. Maybe you could point out where this is
12 required by the claims, this inability to reverse engineer the hash or the
13 encoding.

14 MR. STEPHENS: The claims require that the tokens produced by the
15 encryption server in Claim 7, the identity of the individual has to be
16 unattainable from those tokens.

17 JUDGE GIANNETTI: Okay, so that means that they can never be
18 reverse engineered. Is that correct? Or reversed, I guess that's the term.

19 MR. STEPHENS: That's correct. And that's what's described in the
20 specification of the 641 patent. But that's the problem with the reliance on
21 Settimi's EPIDs. Settimi intentionally created its EPIDs to allow the patient
22 care providers to be able to re-identify the patients. That's why they attach
23 these EPIDs to the records that are released to the central warehouse. So
24 when you run a search on that warehouse, you get back the EPIDs and you
25 can re-identify the patients. There's simply no hash function or any other

1 methodology described in Settimi that would irreversibly deidentify the
2 EPIDs such that the identity of the patient would remain unattainable.

3 JUDGE AMUNDSON: This is Judge Amundson. You're about 41
4 minutes into your initially requested 45.

5 MR. STEPHENS: Your Honors, I'm happy to take any further
6 questions. Otherwise we'll reserve the balance of our time for rebuttal.

7 JUDGE GIANNETTI: Yes, Mr. Stephens, I had some thoughts about
8 Landi, and I would like to hear, briefly, your position. It may not be
9 necessarily responsive and obviously we'll give the Petitioner a chance to
10 respond also on Landi, if they choose to. But just briefly, can you, in the
11 time remaining, can you just tell us what you, what your position is on
12 Landi?

13 MR. STEPHENS: We see at least three deficiencies in the Dick-
14 Landi ground. So the first is that the combination as proposed, fails to meet
15 the claim limitation that requires that the produced healthcare information is
16 absent personally identifying information. So both parties are in agreement
17 that what's produced by this combination, what's returned back to the user in
18 response to a query, includes the encrypted ID as disclosed in Landi. What
19 is that encrypted ID? It's an encrypted form of PII. And that's also not in
20 dispute. At column 5, lines 16 through 19, Landi explains that patient
21 identifying information is encrypted to generate the encrypted ID. So the
22 encrypted ID is thus an encrypted form of PII.

23 Now, Petitioner, we recognize their position that this portion of the
24 data record is reversibly encrypted. So they contend that it is absent PII.
25 But what do the claims require? The claims require production of healthcare
26 information that is, and I quote, absent personally identifiable information.

1 Petitioner contends that the encrypted ID that's returned to the user satisfies
2 this limitation because the unencrypted form of PII cannot be discerned by
3 the recipient without a decryption key.

4 But this position, in our view, is exposed when you look at the claim
5 language again. And we realize that it demands the absence of PII without
6 qualifying its reference to PII. It says, absent PII, not immediately
7 accessible, unencrypted PII. And so in our view, the encrypted ID that's
8 returned as part of the healthcare information in this Dick-Landi
9 combination just fails to meet this limitation of the claim. Second, on slide
10 57.

11 JUDGE MCNAMARA: Counsel, this is Judge McNamara again.
12 Before I get confused, because at the beginning I asked this question about
13 tokenization versus encryption, and now you're telling me encrypted
14 information is, well, I'm not sure what you're telling me about encrypted
15 information in terms of PII. You're saying absent PII. So what's your view
16 now as to both grounds concerning encryption and tokenization?

17 MR. STEPHENS: Well, I think our position, Your Honor, please let
18 me know if you have further questions. I believe our position is consistent.
19 What we have here in Landi, just as in Settimi, is what they've alleged to be
20 a token that's not been hashed. It's not irreversibly deidentified. It can be
21 decrypted to reveal the unencrypted form of that PII.

22 So what's produced in this combination is an encrypted ID that is an
23 encrypted form of PII. And all we're saying is that this fails to meet the
24 limitation of a claim that requires production of healthcare information to be
25 absent PII. The token itself, the encrypted ID is PII. It's just an encrypted

1 form of that PII. So it's not absent. Does that answer your question, or I'd
2 be happy to further --

3 JUDGE MCNAMARA: I don't know that it does, but I guess I'm just
4 going to have to think about it.

5 JUDGE GIANNETTI: Okay. Anything further, Mr. Stephens?

6 MR. STEPHENS: One other, if you wouldn't mind, Your Honors,
7 just one other point about this encrypted ID. I think it's important to note
8 that this encrypted ID is not compliant with HIPAA. So it does go back to
9 HIPAA. But we do have evidence on the record from Petitioner's witness,
10 Dr. Clark, where he contends, he acknowledges that the encrypted ID fails to
11 comply with the requirement in HIPAA for re-identification codes not to be
12 derived from PII. If you're going to use something to re-identify a patient,
13 HIPAA says you cannot do that with PII. But that's exactly what the
14 encrypted ID does in Landi.

15 And again, we look back at the Petitioner's motivations to comply.
16 Why are they bringing in Landi to this combination? It's to comply with
17 HIPAA. And yet, now they're bringing in an aspect of Landi's teachings that
18 are not compliant with HIPAA. So we think this does undermine their
19 motivation to combine as set forth in the petition.

20 And also, we look at dependent Claims 2, 5, and 8. We have an
21 encrypted ID that's been acknowledged by both experts not to comply with
22 HIPAA. It can't meet the limitations of Claims 2, 5, and 8 that require the
23 produced healthcare information to be produced in conformity with HIPAA.

24 JUDGE GIANNETTI: All right. Thank you.

1 JUDGE MCNAMARA: Actually, thank you. That helps me. This is
2 Judge McNamara. Thank you. I think I have a better understanding your
3 position now. Thank you.

4 MR. STEPHENS: Thank you, Your Honors.

5 JUDGE GIANNETTI: Anything further from the panel for Mr.
6 Stephens at this stage? All right, how many minutes does he have left,
7 Judge Amundson? Thirteen or so?

8 JUDGE AMUNDSON: Yes, that's exactly my count. They have 13
9 minutes left for surrebuttal.

10 JUDGE GIANNETTI: All right, thank you very much, Mr. Stephens.
11 Mr. Oliver, you have what, 16 minutes?

12 MR. OLIVER: Thank you, Your Honor. I'll start with the point that
13 was just raised. So start with one thing. Patent Owner admits that the hash
14 function as described in Evenhaim counts as a token within the scope of the
15 claims. So I think that resolves things for Ground Two. Now there seems to
16 be an argument that the reversible or decryptable encryption in Landi doesn't
17 count because according to the Patent Owner, it has to be a type of
18 encryption that can't be reversed. I'll point just to the patent on this, and this
19 is on slide 8 of our demonstratives and it's in the patent at column 5, lines 54
20 to 67.

21 For tokenization, the patent says you can use one or more encryption
22 techniques, for example hash functions and other methodologies. There's no
23 dispute that Landi is an encryption technique. It seems to be Patent Owner's
24 argument of yeah, I know what our patent says, and it says you can use any
25 encryption technique including hash functions. But for purposes of trying to
26 defend ourselves, we're going to say that our claims have to be only

1 irreversible hash functions. That is simply inconsistent with the
2 specification and just for that reason alone, doesn't work. And I think that is
3 the simplest answer to what's being argued here.

4 And I'll add one other point. The Patent Owner's argument seems to
5 be that it doesn't count if it's decryptable because there's still the person's
6 name, John Smith, when the encryption takes place in Landi. You encrypt
7 that or transform that name into something else, but the name's still kind of
8 in there. That would be equally true of a hash function. A hash function
9 takes something and transforms in some way. It seems to be that the Patent
10 Owner is saying, although we didn't limit our claim to only hash functions,
11 please now limit our claim to only hash functions. But that's not what's
12 claimed, it's not what's described in the specification, and it's not a claim
13 construction that's been presented by the Patent Owner. For that reason, we
14 believe that argument is incorrect.

15 So that was the last point raised by the Patent Owner. I'd like to go
16 back to the beginning with their teaching away argument because I think
17 there's a few points to be made on that.

18 The argument goes something along the ideas that Evenhaim would
19 only search the most original raw data and nothing else. What Evenhaim
20 really is talking about is problems with the designs of prior deidentified
21 databases. And there's more than one way you can deidentify something.
22 HIPAA itself has expert determination method, Safe Harbor method. So it's
23 not a one size fits all solution.

24 What the Evenhaim patent complains about is when the deidentified
25 databases aggregate up to what it calls a zip code level, meaning everybody
26 in this zip code, which it talks about at column 1, line 43, or up to the

1 physician level, meaning I'm not going to identify individual patients. I'm
2 going to say all of these diagnoses are by this one doctor. It's the physician
3 level. And that's discussed in Evenhaim at column 17, line 35. And it's
4 provided on slide 16 of our demonstratives.

5 The other example given in Evenhaim and talked about on slide 16 is
6 the age group. It's saying once you do that, you have aggregated up to an
7 entire zip code, you've aggregated up to a physician level, you've aggregated
8 up to an age group. Well, now I can't see the individual records for
9 particular patients, and that's problematic for Evenhaim. Fine.

10 The combination relies on Settimi, which uses a database that's being
11 deidentified in such a manner that the individual records remain. And I
12 would direct the panel's attention on this point to paragraph 38 of Settimi.
13 And the second sentence of that paragraph says the deidentification process
14 removes information that will identify a patient while still retaining
15 clinically useful information about the patient. And I think a little bit, and I
16 hate to go back to HIPAA again, but because it keeps getting raised, I think
17 some clarity would be in order here.

18 The Patent Owner's argument is, well, if Settimi's database is
19 deidentified in conjunction with HIPAA, then all bets are off. Nothing
20 works for purposes at Evenhaim. I would simply direct, and I don't want to
21 burden the panel with getting into HIPAA, but I will note that Exhibit 2006
22 provides the HIPAA rules which says you can do the expert determination of
23 deidentification or the Safe Harbor where you remove certain pieces of
24 information. Those pieces of information are things like the name, the fax
25 number, the date of birth, the zip code, whatever the case may be.

1 Evenhaim is interested in finding a specific patient's record. If Settimi
2 associates that person's healthcare record with a token that identifies that
3 person, who cares that you no longer know the fax number of that patient?
4 Who cares that you no longer know the Social Security number of that
5 patient? If Evenhaim just wants to find the patient record, Settimi's database
6 allows that regardless of whether or not the fax number for that patient is no
7 longer there. Because what Settimi explains is that I'm just taking away
8 what identifies the person, but I'm leaving in place a token so you can still
9 find that record if you want to. And as we discussed earlier, and I won't
10 rehash this too much, Evenhaim describes that at the aggregator you can
11 perform tokenization there and you can search by name, ID or the like.
12 Whatever terminology is used by the databases you're searching is what you
13 do.

14 Evenhaim describes that you're going to search for a record. Settimi
15 allows for you to find that record. That's all that's needed. And it's really
16 nothing more than that. And this whole idea that Settimi has been
17 deidentified because the fax number or the name or the date of birth is no
18 longer there. If you can find the patient's record, what do you care about
19 anything else? And the answer is Evenhaim wouldn't care. And for that
20 reason I think the Patent Owner's arguments are just a little bit of
21 misdirection.

22 And I'll note just again, I've made this clear before, but on slide 24 of
23 our demonstratives, Settimi specifically says that a user may search by EPID
24 number. I know the Patent Owner is going to say well, that particular
25 discussion was given for another database. But the point is the design of
26 Settimi allows for searching of particular tokens and an EPID is nothing

1 more than a token. If that's allowed in the database and it's a searchable
2 term, and we know Evenhaim says that you can create a token at the
3 aggregator side, then there doesn't seem to be any problem. And for that
4 reason we believe the teaching away just simply does not make sense.

5 I'll note too that the Patent Owner raised this idea of Evenhaim's use
6 of identity-free microdata and the argument that that microdata that's been
7 deidentified as later in the process. Patent Owner misses the point of the
8 argument. The point of the argument of raising Evenhaim's discussion of
9 identity-free microdata is, and we can see this from Patent Owner slide 12,
10 from their arguments on the right, and I won't go into it in detail, but
11 essentially their argument is that Evenhaim is interested in the microdata,
12 and that's what's key. Our point in raising identity-free microdata, the
13 terminology used in Evenhaim, makes clear that the identity of the person is
14 separate and apart from the microdata. If you're interested in the microdata,
15 and Evenhaim says you can have identity-free microdata, then the identity is
16 not important. The records are. Evenhaim wants to know does this person's
17 records indicate that they have high blood pressure? Does this indicate that
18 they have some chronic disease? Evenhaim searchers are insurance
19 companies. They want to know what's in the records. They want to know
20 illnesses, whether or not they're taking their blood pressure medication,
21 whatever the case may be. And that's allowed by Settimi's system because it
22 maintains the original healthcare records even if it takes off the name and
23 Social Security number.

24 I'll also note with respect to the combination of Evenhaim and Settimi
25 that the motivation to combine in part is that they're both directed to the
26 same ideas, which is providing deidentified databases and providing answers

1 to people who want to pure query medical records. But also, and this is
2 discussed in slide 19, another reason for the combination is it simply
3 simplifies the query. While Evenhaim's system had to go out to maybe 10 or
4 20 different databases and search each one using the same query over and
5 over again, Settimi says I'm going to put all that information together for you
6 in one centralized database. And one centralized database is easier to search
7 because you only have to do the search once. That is an independent reason
8 for the combination that the Patent Owner seems to set aside.

9 With respect to, I know the Patent Owner brought up, or Counsel
10 brought up Claims 2, 8 and 18, which specifically call for HIPAA
11 compliance. I think the simplest answer to that is one I've given already,
12 which is, well, first and foremost that has not been separately briefed by the
13 Patent Owner. They have not made arguments as to those specific claims. I
14 will note, however, that those claims just leave it to the person of skill to do
15 whatever is needed to comply with HIPAA. There's nothing in those claims
16 that says, by the way, here's the trick that you have to do. Again, HIPAA is,
17 in part, using expert knowledge to provide scientific principles to make it as
18 safe as reasonably possible so that the risk is small.

19 The patent leaves that to the POSA to do because the POSA can put in
20 whatever safeguards and measures that are available at the time as needed.
21 And the person of ordinary skill in the art looking at Evenhaim and Settimi
22 would use the same level of care as they would looking at the claims of the
23 641 patent that just say hey, by the way, comply with HIPAA.

24 To the extent it's necessary, because I know the Patent Owner brought
25 up the whole idea of what HIPAA rules allow for. I will just note that
26 Exhibit 1016, which is a record of pages 30 to 31, does indicate that

1 reidentification is not only permissible, but things like hash functions are not
2 problematic for purposes of reidentification, which is what Settimi uses.

3 Apart from that, with respect to the combination and the argument that
4 Settimi's manner of using a hash function is somehow different than
5 Evenhaim's and different than what the patent talks about and therefore
6 doesn't work, I will note that that paragraph of Settimi that is raised, give me
7 one moment, in our demonstratives on slide 23, where there's a citation to
8 Settimi at paragraph 41. The example given in Settimi is using these EPIDs,
9 which use a hash function. But it also says in paragraph 41 that other
10 methods are available.

11 For purposes here, it doesn't matter what method you select for
12 tokenization. Evenhaim talks about just using a hash. Evenhaim talks about
13 these PIDs plus a hash. Because Settimi says hey, use whatever you want,
14 that disclosure of Evenhaim, to the extent the Patent Owner thinks it's
15 problematic and that someone would want to do something different, Settimi
16 allows for that. You can use whatever method of tokenization you want if
17 that would make you feel more comfortable because you're worried about
18 some HIPAA compliance issue. So I think that addresses the arguments
19 concerning the combination of Evenhaim and Settimi.

20 I will note that Counsel brought up the idea that in Settimi only the
21 database knows how to create EPIDs. Again, this is attacking the references
22 individually. We rely on Evenhaim for the idea of an encryption server,
23 which is the aggregator in the middle. We rely on Evenhaim for the idea
24 that that thing can search by whatever is needed in the database. It can have
25 a manner of generating a token if needed, and if you're concerned about that,
26 it can have an escrow agent that holds the keys so that that can't be used. So

1 we rely on Evenhaim for the idea that there is an encryption server, that that
2 encryption server can perform tokenization. So attacking Settimi alone on
3 the idea that that database isn't described as sharing the key with something
4 else isn't really the point, because we are relying on Evenhaim for much of
5 the other parts of the claim. Absent any questions from the panel, I think
6 I've covered everything I wanted to. I'm happy to answer any questions, but
7 other than that, I'd be happy to concede the rest of the time.

8 JUDGE GIANNETTI: Okay, Mr. Oliver. I have nothing further.
9 Panel?

10 MR. OLIVER: Thank you.

11 JUDGE MCNAMARA: Nothing from Judge McNamara.

12 JUDGE GIANNETTI: Okay, thank you very much, Mr. Oliver. And
13 we will have a brief surrebuttal from Mr. Stephens. Thirteen minutes. You
14 can proceed.

15 MR. STEPHENS: Thank you, Your Honor. I'd just like to return to
16 the point on the role of HIPAA in the grounds that have been raised in the
17 petition. Mr. Oliver mentioned that HIPAA keeps getting raised by Patent
18 Owner. But HIPAA was the only basis for motivations offered by the
19 Petitioner. It's foundational to the assessment of their advanced motivations
20 to combine in the petition for both Evenhaim and Settimi and the Dick and
21 Landi combination. HIPAA is in the backdrop of whether a person of skill
22 would have, not just could have, combined the references, but would they
23 have motivation to integrate Settimi's warehouse into Settimi? Would they
24 have motivation to combine Dick and Landi as proposed?

25 And just don't take my word for it. If we look at the petition, I'll just
26 give you a few cites. Pages five to six. The petition starts with two pages of

1 discussion of state of the art and what they're explaining the state of the art is
2 HIPAA. That's their starting point for the analysis in the petition. Then you
3 look at page 37. The motivation for integrating Settimi into Evenhaim is
4 born out of HIPAA. They mentioned HIPAA, I don't have an exact count,
5 but three or four times at least through that discussion of the overview of the
6 combination. Same with the Dick-Landi grounds, pages 57 through 60.

7 You'll see HIPAA at least four times through that discussion, emphasizing
8 the importance of complying with HIPAA in addressing multiple claim
9 limitations. So we bring forward HIPAA issues in our briefing because the
10 Petitioner framed its own combinations in terms of HIPAA compliance.

11 With HIPAA applicable, again we look at whether the tokens that
12 have been proposed to produce in both combinations would be HIPAA-
13 compliant. Neither Settimi's nor Landi's tokens are HIPAA-compliant.
14 They're not irreversibly deidentified. There's been no disclosure identified
15 by the Petitioner that suggests that Landi's encrypted ID would ever be
16 irreversibly deidentified. You search through Landi, there's no discussion of
17 irreversible deidentification of the encrypted ID, no hashing in Landi. And
18 that makes sense because the background discussion in Landi, what Landi
19 was trying to achieve was reidentification. For reidentification, you can't
20 have something that's been irreversibly deidentified. But that's what they
21 brought into the combination. And so because of that, these tokens are not
22 HIPAA-compliant. We think that does undermine the motivations set forth
23 in the petition. And then as to Dependent Claims 2, 8, and 15, our Patent
24 Owner's response focused on a lot of the deficiencies in these combinations
25 as it pertains to HIPAA. And so we did contend in our briefing there that

1 these combinations are not HIPAA-compliant, which is exactly what Claims
2 2, 8, and 15 require. Happy to take any further questions, Your Honor.

3 JUDGE GIANNETTI: Panel, any further questions?

4 JUDGE MCNAMARA: Just one about this HIPAA compliance stuff
5 and reidentification. And this has to do with Landi. I'm just looking at
6 Landi's abstract, and he says the purpose of this is to ensure patient privacy.
7 Deidentifying patient data to ensure patient privacy while allowing only the
8 owners of the patient data and/or legally empowered entities to reidentify
9 subject patients associated with deidentified patient data records. So how is
10 that not HIPAA-compliant?

11 MR. STEPHENS: Yes, Your Honor. It's a great question. So
12 HIPAA prevents the release of any reidentification code for any purpose if
13 it's not been irreversibly deidentified. And that's what we established, not
14 just from Dr. Rubin, our expert, but also during the deposition of Dr. Clark.
15 And I'll direct Your Honors to a slide. The language of the HIPAA rule is
16 quite clear about this.

17 JUDGE MCNAMARA: Yes, notwithstanding the HIPAA rule, I
18 mean, I understand that. I don't need a lot of documentation on that. But I
19 guess as I read that abstract, it says systems and methods are provided which
20 implement secured key encryption for deidentifying patient data to ensure
21 privacy while allowing only the owners of the patient data and/or legally
22 empowered entities to reidentify the subject patients associated with the
23 deidentified patient data. That sounds like the objective is a HIPAA
24 objective. Are you suggesting perhaps that Landi doesn't accomplish that?

25 MR. STEPHENS: Yes, Your Honor. That's what the record bears
26 out, actually.

1 JUDGE MCNAMARA: Okay.

2 MR. STEPHENS: Despite the representation in Landi, it's incorrect.
3 And Dr. Clark conceded as much during his deposition. Slide 57 provides
4 the HIPAA rule. You cannot release these types of reidentifiable codes as
5 described in Landi. It's not compliant with HIPAA and both experts are in
6 agreement on that point.

7 JUDGE MCNAMARA: All right, so Landi doesn't achieve the
8 objective that's in that abstract as I read it. Is that right?

9 MR. STEPHENS: Yes. And just one more point to that. We raised
10 this issue in our Patent Owner's response. What did we see back from the
11 Petitioner in their reply and in Dr. Clark's second declaration? He didn't
12 rebut the point. We asked him if he had independently analyzed it, gone
13 back to the rule. He said no. He just said a person of skill in the art would
14 have no reason to doubt Landi's disclosure.

15 JUDGE MCNAMARA: Okay. Thank you very much. I appreciate
16 it.

17 JUDGE GIANNETTI: Anything further from the panel? All right. I
18 think that wraps things up. Well, I want to thank counsel for their
19 preparation. I think this has been a very helpful argument. And we'll take
20 your case under submission. I will ask you to stay on the line with the court
21 reporter for any questions that the reporter might have on spellings, et cetera.
22 Otherwise, we're adjourned. Thank you very much.

23 (Whereupon, the proceedings at 4:01 p.m. were concluded.)

IPR2024-00226
Patent 9,118,641 B1

PETITIONER:

Justin Oliver
Nicholas Marcello
VENABLE LLP
joliver@venable.com
ndmarcello@venable.com

Michael Sandonato
msandonato@fchs.com

PATENT OWNER:

W. Karl Renner
Jeffrey Barclay
Nicholas Stephens
FISH & RICHARDSON P.C.
axf-ptab@fr.com
barclay@fr.com
nstephens@fr.com