Trials@uspto.gov
571-272-7822

Paper No. 43
Entered: March 20, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00212 (Patent 11,178,116 B2)
IPR2024-00214 (Patent 11,068,609 B2)
IPR2024-00215 (Patent 10,452,854 B2)

Record of Oral Hearing
Held: February 27, 2025

Before THOMAS L. GIANNETTI, JASON M. REPKO,
STEPHEN E. BELISLE, and DANIEL KAZHDAN,
Administrative Patent Judges.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

GREG NIEBERG, ESQ.
Wolf Greenfield
605 Third Avenue
25th Floor
New York, NY 10158
(212) 697-7890

ON BEHALF OF THE PATENT OWNER:

NATHAN LOWENSTEIN, ESQ.
Lowenstein & Weatherwax LLP
1016 Pico Boulevard
Suite 3200
Houston, TX 77002
(310) 307-4502
lowenstein@lowensteinweatherwax.com

ANDREI IANCU, ESQ.
HALEY SANDERS, ESQ.
Sullivan & Cromwell LLP
1700 New York Ave NW #700
Washington, DC 20006
(310) 712-6600 (Iancu)
(212) 558-4000 (Sanders)
iancua@sullcrom.com
sandersh@sullcrom.com

The above-entitled matter came on for hearing on Thursday, February 27, 2025, commencing at 1:00 p.m., via video teleconference.

1 P R O C E E D I N G S
2 - - - - -
3 JUDGE GIANNETTI: Welcome everyone. Welcome to the
4 PTAB. This afternoon we have a consolidated hearing in three inter partes
5 review proceedings. And I'll read them off, IPR2024-00212, IPR2024-
6 00214, and IPR2024-00215. The patents involved are patent 11,178,116,
7 that's in the 212 proceeding; in the 214 proceeding, it's 11,068,609; and in
8 the 215 proceeding, it is 10,452,854. The caption of all of these cases is
9 Google LLC versus Security First Innovations.
10 I'm Judge Giannetti. I will be presiding at this afternoon's hearing.
11 We also have our other panel members, Judge Belisle, Judge Repko, and
12 Judge Kazhdan.
13 I want to point out – as I said in the order -- that this is not an
14 expanded panel. Judge Kazhdan is paneled only on the 212 case, and Judge
15 Repko is not paneled on that case. So this is not an expanded panel. With
16 that, let me get your appearances, Counsel. Let's start with the Petitioner.
17 MR. NIEBERG: Good afternoon. My name is Greg Nieberg on
18 behalf of Petitioner Google. I'm joined by my colleagues, Dr. Elisabeth
19 Hunt and Richard Giunta. And I'll be arguing all three matters today for
20 Google.
21 JUDGE GIANNETTI: Okay.
22 MR. IANCU: And good afternoon, Your Honors. Andrei Iancu
23 from Sullivan and Cromwell on behalf of Security First Innovations, also
24 known as SFI. With me from Sullivan and Cromwell is also Stephen Elliott
25 and Haley Sanders. By the way, Ms. Sanders is going to be arguing at her

1 very first hearing in her career in any court. So she is a LEAP practitioner.
2 And also with us are three attorneys from the Lowenstein and
3 Weatherwax firm. First, Mr. Nathan Lowenstein, Kenneth Weatherwax, and
4 Colette Woo. We're going to have three attorneys arguing, myself as well as
5 Mr. Lowenstein, and as I've mentioned, Ms. Sanders. Thank you.
6 JUDGE GIANNETTI: Okay. All right. Thank you. We have
7 quite a crowd here for these proceedings. So let me give you a little bit of
8 instructions. I'm sure you are familiar with our procedures here. But I just
9 wanted to give you a few ground rules for the case.
10 First of all, we want to make sure that you have a right to be heard.
11 And we want to make sure that that's fulfilled. If you have any problems,
12 technical problems -- we don't expect any, these usually run very smoothly.
13 But if there are any technical problems, you get cut off or something is
14 wrong with your connection, please let us know, let our tech team know.
15 And we'll get you back online as soon as we can.
16 When you're not speaking, we would appreciate it if you would
17 mute yourself. If you haven't spoken for a while, please identify yourself
18 before you speak. We'll try to do the same.
19 We have the whole record in the case. We have all of your filings.
20 And we also have your demonstratives. So if you do refer to -- I assume you
21 will be referring to the demonstrative during your proceeding. You can
22 either present them by sharing your screen, that's one option. Or if you
23 prefer, you can just give us the slide number, and we will look them up in
24 our files. I think that in either case, you should give us the slide number so
25 that the record shows what you are referring to.

1 We did get a motion from the -- I believe it was from the Patent
2 Owner. We got a motion from the Patent Owner objecting to the Petitioner's
3 demonstratives. First of all, I'm going to tell the parties, remind you, that the
4 demonstratives are not evidence in this case, in any case. And so we will
5 consider your objections.
6 But I want to warn you, caution you, that any arguments that are
7 not in the papers, we will not credit. So please limit your arguments to
8 evidence and arguments that have been made in the papers. No new
9 arguments, no new evidence, whether they're in demonstratives or whether
10 they're in your argument.
11 And I just wanted to check -- and perhaps during your presentation
12 you can tell us -- whether there was a meet and confer concerning these
13 objections to demonstratives. If you read our pretrial order, we do require a
14 meet and confer, to try to resolve any problems with the demonstratives
15 before they're presented at the trial hearing. So I would like you to confirm
16 that that a meet and confer took place. If it didn't take place, we may not
17 consider your objections.
18 Let me see if I have anything else here. We realize that you have a
19 LEAP practitioner. And we welcome Ms. Sanders to the proceeding. Each
20 side will get two hours. And the Patent Owner will get an additional 15
21 minutes, for a total of two hours and 15 minutes. The Petitioner may reserve
22 time for a rebuttal case. The Patent Owner may also reserve the time for
23 surrebuttal. And I will ask each party at the beginning of their presentation
24 how much time they reserve for rebuttal or surrebuttal.
25 We will not stop you from going into your rebuttal time. We will

1 keep time, obviously. Judge Kazhdan will be assisting me in keeping time.
2 And we don't have a visible clock in these virtual proceedings. But we will
3 try to keep you on schedule by giving you a warning when you get to the
4 end of your allotted time.
5 If you want to continue -- as long as you are within the 2 hours and
6 15 minutes, if you want to continue into your rebuttal or surrebuttal time,
7 you're free to do that. But it will come out of your time. We will try to give
8 you warnings when you're close to the limit and when you're at the limit.
9 The Petitioner will go first and followed by the Patent Owner, then
10 the Petitioner's rebuttal, Patent Owner's surrebuttal. And they will have 2
11 hours and 15 minutes. And I will ask you to stay on the line when we're
12 done. The panel will sign off at the end of the hearing. But let's stay on the
13 line in case the court reporters have any questions about spellings, et cetera.
14 Court reporters have your demonstratives, but there may be some
15 spelling issues and issues about your argument, the details of your argument,
16 and pronunciations and spellings that will be dealt with after the hearing.
17 Any questions before we begin, Petitioner, any questions?
18 MR. NIEBERG: No, Your Honor. I'll be calling out the slide
19 numbers, not presenting them.
20 JUDGE GIANNETTI: You'll be calling them out. You won't be
21 sharing your screen?
22 MR. NIEBERG: Correct.
23 JUDGE GIANNETTI: Okay. That's fine. We can handle that.
24 Any questions from the Patent Owner?
25 MR. IANCU: No questions, Your Honor. Just to alert the panel as

1 well as everybody else on the Zoom, everybody on the Patent Owner's side
2 is in one room and I am just now standing at the podium. So during
3 Petitioner's argument, I'll be leaving the podium. I didn't want you to think
4 that we're not here. We are here. But the camera is at the podium where
5 there's -- I'm not going to stand the whole time during the argument, if that's
6 okay.
7 JUDGE GIANNETTI: Understood. That's fine. Yes.
8 MR. IANCU: Thank you. And to answer Your Honor's question,
9 there was a meet and confer. And Petitioner did revise some slides in light
10 of the meet and confer, just a few, refused to revise the others. But that did
11 happen.
12 JUDGE GIANNETTI: All right. Fine. Well, then my statement
13 that we will defer consideration of your objections will stand. Thank you for
14 that information.
15 MR. IANCU: Thank you.
16 JUDGE GIANNETTI: I think we're ready to begin. Let's begin --
17 start with the Petitioner. Petitioner's Counsel, do you want to reserve time
18 for rebuttal?
19 MR. NIEBERG: Yes. I'd like to reserve 30 minutes for rebuttal.
20 JUDGE GIANNETTI: All right. Whenever you're ready, you
21 may begin.
22 MR. NIEBERG: Great. Good afternoon. I'm on Slide 3. Slide 3
23 shows the order I plan to discuss the various grounds. I've organized, based
24 on ground, because there is some overlap across the petitions. And so I may
25 jump between the proceedings a little.

1 I'll start with the Tajima Grounds 1 and 2 for the '116 patent, the
2 212 proceeding. I'm on Slide 7 now. Claim 1 is on the left of Slide 7. I'm
3 going to focus on Claim 1 because the disputes are identical for the two
4 independent claims. Claim 1 distributes a data set into portions called data
5 chunks in 1A. Then each chunk is encrypted with its own encryption key in
6 1B.
7 Next, each key is obfuscated in 1C. An example of obfuscation is
8 pairing each chunk with another chunk's key. So, for example, chunk 1's
9 key is paired with chunk 2, and chunk 2's key is paired with chunk 3 and so
10 on.
11 Finally, each chunk and key pair is stored on different storage
12 devices in 1D. For Ground 1, we had anticipation and obviousness
13 arguments. I'm going to focus on obviousness because the argument is
14 straightforward and the corroborating evidence we cited in support is clear.
15 Slide 11. On the right of Slide 11, Tajima has a data set of
16 personal information in orange, like a username or an e-mail. Tajima
17 describes that in paragraph 6. Tajima distributes the personal information
18 into two data fragments, X and Y in blue. The data fragments are the
19 claimed data chunks. Each data chunk is encrypted with its own encryption
20 key, which is described in the blue text in the middle of Slide 11.
21 Next, Tajima obfuscates the key information in the same way the
22 patent obfuscates its keys. Chunk X is paired with chunk Y's key
23 information and vice versa. That's in the red highlighted text and shown in
24 Figure 13. Finally, each chunk plus key information pair is stored in a
25 different storage device. So those are the purple databases in the bottom

1 right on Slide 55. None of that is disputed.
2 The only dispute is about the language that we underlined in the
3 bottom left of Slide 11 in limitation 1D. The dispute is whether a person of
4 ordinary skill -- a POSA, as I may refer to it -- would have found it obvious
5 to store Tajima's encryption key with the data chunk.
6 Slide 12. Storing Tajima's keys with the data chunks was obvious.
7 Slide 12 shows 4 pieces of corroborating evidence we cited that prove that
8 storing a piece of encrypted data with an encryption key, including with an
9 obfuscated encryption key, was part of a POSA's background knowledge.
10 For example, Orsini in the middle of Slide 12 and Exhibit 1113, on
11 the right side of Slide 12, each key storing obfuscated keys with encrypted
12 pieces of data. It's not shown on Slide 12, but Foster and Exhibit 1113 even
13 use the term key information, the same term used in Tajima to represent data
14 that includes the corresponding encryption key.
15 You can see that -- you can see where -- Foster discloses that on
16 Slide 13, if you're interested. And Exhibit 1113 says that, it's paragraph 98,
17 which our reply discussed at page 9. There's no dispute that the evidence on
18 Slide 12 is part of a POSA's background knowledge. And it demonstrates
19 that it was known to store encryption keys with encrypted pieces of data.
20 Slide 15. A POSA's motivation to use the known technique of
21 storing encryption keys with encrypted data in Tajima is straightforward.
22 Both experts agree that Tajima's encryption keys must be stored somewhere.
23 You can see that testimony from SFI's expert, Dr. Rubin, on Slide 16.
24 SFI's expert testified that Tajima allegedly doesn't go into the
25 detail of where those keys are stored. If that's true -- and what that means is

1 Tajima is open to any known way of storing its encryption key. As I
2 demonstrated on Slide 12, there's no dispute that one known conventional
3 way to store encryption keys, including obfuscated key, is with the
4 encrypted -- with encrypted data chunks.
5 But our petition didn't stop there. We didn't just prove it was
6 known and conventional. We demonstrated that storing keys with data was
7 a beneficial design choice for Tajima. Dr. Bhattacharjee explained in
8 testimony on the left of Slide 18 that a POSA would have recognized
9 benefits in storing Tajima's keys with the data chunks.
10 For example, it would have avoided the need for additional key
11 infrastructure and key management. So when keys are stored separately
12 from the data, you need an additional key storage device to store the keys
13 and some additional key management to retrieve and keep track of where
14 those keys are stored.
15 JUDGE GIANNETTI: Counsel, this is Judge Giannetti. Wouldn't
16 it be more secure? Would it be more secure to store the key separately?
17 MR. NIEBERG: Separately, you mean in a totally entirely
18 different data location?
19 JUDGE GIANNETTI: In a different location.
20 MR. NIEBERG: Well, I don't know if it would be more secure. I
21 think it depends on what types of attack you're trying to prevent against.
22 JUDGE GIANNETTI: Yes.
23 MR. NIEBERG: But -- and what you're -- the value of your data is
24 what you're more interested in versus -- so let me take a step back. Our
25 argument is that when you store it with -- the keys with the data is that it

1 simplifies the key management. It's more efficient. So when you pull the
2 keys and -- pull the data chunks, the keys come along with it. So there's an
3 efficiency and benefit to doing it.
4 So even if there were some potential security deficiencies in some
5 situations, there are still known benefits to doing our obvious modification
6 of storing the keys with the data chunk.
7 JUDGE GIANNETTI: I guess what I'm asking is in Tajima,
8 wouldn't storing the key separately from the key information provide another
9 level of security?
10 MR. NIEBERG: Well, our position is that Tajima is disclosing
11 storing the keys with the key information. But for the obviousness
12 argument, again, I think it depends on -- so if you're storing the key
13 somewhere else, it depends --
14 JUDGE GIANNETTI: Yes.
15 MR. NIEBERG: -- of course on the security of that other location.
16 If it's a poorly stored location, then you're not getting much benefit. But
17 even if it's a very secure --
18 JUDGE GIANNETTI: Look, I assume that if you're going to go
19 through the effort of storing the key separately, you would make sure that it
20 was stored in a separately secure location, right?
21 MR. NIEBERG: You would think so if it was well designed. We
22 don't dispute that there are ways --
23 JUDGE GIANNETTI: There are ways to do that, right?
24 MR. NIEBERG: Of course. There are always ways to add
25 security. It's always a trade-off, a balance between efficiency, speed, and the

1 type of data you're trying to secure. Did I answer your question?
2 JUDGE GIANNETTI: Yes, I think so. But in Tajima, you're not
3 storing the key with the data to which it applies; is that right? Even under
4 your theory, there would still be this obfuscation as you put it, where the key
5 for Y would be stored with X and the key for X would be stored with Y
6 under your view; is that right?
7 MR. NIEBERG: Well, for Ground 1, yes, that -- the Tajima
8 teaches obfuscation. So both in our obviousness case and our anticipation
9 argument --
10 JUDGE GIANNETTI: Right.
11 MR. NIEBERG: -- the keys are swapped.
12 JUDGE GIANNETTI: So what difference does it make if you
13 have to look elsewhere for the key? Whether you look to another data
14 fragment or if you look to some other storage area, what difference does it
15 make? You still have to look someplace else for the key.
16 MR. NIEBERG: So, as Dr. Bhattacharjee testified, and there's no
17 dispute, that it does simplify the key management. Because when you're
18 pulling the data chunks, you're pulling the keys as well. And then it's just a
19 simple swapping of the keys and data.
20 Where if you could imagine you have thousands and millions of
21 personal information, so two keys per personal information -- so that's 2
22 million keys -- you have to keep track of where all 2 million keys are for all
23 2 million pieces of personal information.
24 And so when you pull the data chunks, you also have to pull the
25 keys. And you have to do some further processing to figure out how to map

1 that key information -- if it's not the key -- to where the keys are stored.
2 JUDGE GIANNETTI: Will the argument be different for your 103
3 ground?
4 MR. NIEBERG: For Ground 1?
5 JUDGE GIANNETTI: For Ground 2.
6 MR. NIEBERG: Oh, for Ground 2, the keys are stored with the
7 data chunk, but they're also further encrypted by another key.
8 JUDGE GIANNETTI: But they would be stored with the proper
9 data chunk to which they apply; is that right? In that model, your 103.
10 MR. NIEBERG: No. Well, it could be either way. We didn't
11 argue that you would take away Tajima's obfuscation because it does
12 provide some benefit. But we didn't have to demonstrate that there were
13 obfuscation. But we kept the obfuscation there, and they were further
14 secured.
15 JUDGE GIANNETTI: So in either 102 or 103, in your first or
16 second ground, you would still have to look elsewhere for the key for a
17 particular data chunk; is that right?
18 MR. NIEBERG: Well, I don't -- I'm not sure -- if I understand
19 your question, when -- the point is when you pull the data chunks to the
20 place where you want to restore the data, those keys come along with it. So
21 you don't have to look elsewhere to try and find where they are.
22 JUDGE GIANNETTI: But it isn't right there with the fragment,
23 it's someplace else.
24 MR. NIEBERG: Well, it's with both the fragments and -- it's with
25 another fragment for that pair of fragments. And when you pull them both,

1 the keys come along with it, which is simpler, more efficient that Dr.
2 Bhattacharjee explained. And there's no dispute about that than compared to
3 having some additional key management and key infrastructure.
4 JUDGE GIANNETTI: Okay. Thank you.
5 MR. NIEBERG: Okay. So as I just mentioned, SFI did not
6 dispute that we identified known benefits of storing key for data chunks.
7 And as I discussed on Slide 12, that was a known technique. So clearly, a
8 person of skill in the art will recognize that there were some reasons to
9 sometimes store keys with data chunks, including with obfuscated chunks as
10 Dr. -- sorry, Judge Giannetti was asking about. That was known. It was
11 done in the prior art.
12 So what does SFI dispute? That's on Slide 18. SFI has two
13 arguments. First, they argued that the limitation of storing keys with
14 encrypted data was a missing limitation in the prior art and common sense
15 can't be used to fill that gap. Second, SFI argues that storing a key with data
16 entails some risk and was complex.
17 So I'm going to start with the missing limitation argument first. If
18 you look back at Slide 12, as I just mentioned, we have four pieces of
19 corroborating evidence that each taught storing keys with encrypted pieces
20 of data and they -- and a couple of them, at least Foster in Exhibit 1113,
21 stored the encrypted keys in an obfuscated form with the data chunks. That
22 evidence is not in dispute. So this is not a missing limitation case.
23 So how did SFI respond in their sur-reply? Slide 21. On the left of
24 Slide 21 is all SFI sur-reply had to say for obviousness for Ground 1. SFI
25 doesn't dispute that the evidence I showed you on Slide 12 that demonstrates

1 storing keys with encrypted data, including obfuscated keys, was known and
2 conventional. Instead, SFI makes a legal argument. They argue that
3 evidence of a POSA's background knowledge had to be named in Ground 1
4 to be part of the ground.
5 But that's not the law. The Federal Circuit rejected that exact
6 argument in the Philips v. Google case, which is shown on the right side of
7 Slide 12. There, the court affirmed a Board's decision of one reference
8 obviousness that was combined with a POSA's background knowledge that
9 was corroborated by a reference, but that reference itself was not named in
10 the ground. So SFI has the law wrong.
11 This is not a missing limitations case. There's no gap in the prior
12 art that we tried to fill with bare common sense. Instead, we showed that
13 storing keys with encrypted pieces of data was part of POSA's background
14 knowledge and as demonstrated, for example, by the four pieces of prior art
15 I've showed on Slide 12. And that is why they're --
16 JUDGE KAZHDAN: Can you just explain the difference? So,
17 like, I understand that POSA's knowledge could be used to interpret. And
18 that seems like very much an easy case under Koninklijke in particular.
19 But when you started saying that the -- like, that this key would be
20 stored this way, it sort of seems more like you're combining references. And
21 that already seems more like a ground that should have been named in the
22 ground. But maybe you could just elaborate on the law a little bit more.
23 MR. NIEBERG: Sure. And like I said, this was exactly the
24 argument that was raised in the Philips v. Google case, where there was a
25 one reference obviousness case and they proposed a modification based on a

1 POSA's background knowledge. And to demonstrate that background
2 knowledge, they cited one piece of corroborating evidence. We cited
3 multiple pieces of corroborating evidence to show how pervasive it is in the
4 art.
5 But in the Philips v. Google case, they cited just one piece of
6 corroborating evidence. It wasn't named in the reference. On appeal or at
7 the Board, the Patent Owner made the argument he just made as that should
8 have been in the ground, that's -- you're combining or you're modifying.
9 And the Board rejected that argument. And the Federal Circuit
10 affirmed that argument that a POSA's background knowledge, you always
11 view obviousness in light of that. And when you have a single reference
12 obviousness, that background knowledge doesn't have to be named in the
13 ground.
14 And when it's corroborated by evidence, it reinforces that there's
15 not a missing limitation, that we're not relying on bare common sense, we're
16 not making it up. We demonstrated with multiple pieces of evidence that
17 this limitation was just pervasive in the art. Does that answer your question?
18 JUDGE KAZHDAN: Maybe. I'm not -- so I'm just not sure if in
19 that Philips case that was in the petition or was that only in the reply where
20 they started saying let's use a modification based on general --
21 MR. NIEBERG: It was I believe -- it was in the petition. There
22 was -- I believe the Board may have tried to turn it into a combination. And
23 that was improper. They created a ground. But the Board said and the
24 Federal Circuit said you don't have to do that. The corroborating evidence to
25 demonstrate the single reference obviousness, that was in the petition and

1 that ground was valid.
2 JUDGE KAZHDAN: All these cites -- were all these cites in your
3 petition? Like, were you making the same argument that you could use
4 these other references to teach you how to store the keys in the petition or
5 was that -- did that come later?
6 MR. NIEBERG: We made the argument petition that this was part
7 of a POSA's background knowledge. And we argued -- so we had
8 corroborating evidence to show it was part of the background knowledge.
9 And then we had argument with support from our expert, Dr. Bhattacharjee,
10 that there also were benefits to it. So it's not just a known technique type
11 argument. It was known and there were reasons for doing it.
12 JUDGE KAZHDAN: Okay. Thank you.
13 MR. NIEBERG: Great. Okay. So before I move on from Slide
14 12, SFI sur-reply suggests that we only cited one reference by their inventors
15 to demonstrate POSA's background knowledge that storing keys with data
16 was known. SFI is referring to the Orsini reference, Exhibit 1005, which I'll
17 return to later. Three of the exhibits we cited on Slide 12 are not by SFI
18 inventors. So even if Your Honors ignored Orsini, we still prove that there's
19 no missing limitation here.
20 But you also shouldn't ignore Orsini. There's no dispute that
21 Orsini is prior art and proves that a POSA's background knowledge included
22 storing obfuscated keys with encrypted data chunks. So there's no missing
23 limitation.
24 I'll now turn to SFI's second argument, Slide --
25 JUDGE BELISLE: Counsel, this is Judge Belisle. Let's assume

1 that, yes, the skilled artisan knew. I mean, as your evidence is -- you're
2 saying shows that encrypting these individual keys with a key-encrypting
3 key -- which almost by definition is that's what it does. If it's a key-
4 encrypting key, it's going to be used to encrypt keys. So let's assume that
5 that's a given at the time of the invention.
6 In view of Orsini alone, why would that skilled artisan have taken
7 that knowledge and modified Orsini to come up with the challenge claim
8 when Orsini itself, which is -- has multiple -- probably more than skilled
9 artisans involved with that disclosure didn't go there?
10 MR. NIEBERG: So respectfully, Your Honor, that's our Ground
11 2, where we combined with Foster for the key encryption key that you
12 referred to. Our Ground 1 is just about storing the key with the data chunk.
13 It doesn't exclude further encrypting it. But it doesn't require it because the
14 claim doesn't require it.
15 So we didn't address in Ground 1 the additional security of
16 encrypting keys with the key encryption key. That's our Ground 2 in the
17 '116. And that's also our Ground 1 in the '609 and '854 patent. So I'd be
18 happy to answer your question, but it might make more sense when I turn to
19 Ground 2.
20 JUDGE BELISLE: Sure.
21 MR. NIEBERG: If it comes up again.
22 JUDGE BELISLE: Let's wait.
23 MR. NIEBERG: Okay. So on Slide 23 now. So SFI's second
24 argument was that storing keys with encrypted data could have security
25 drawbacks -- I think what Judge Giannetti was referring to. And so that

1 argument fails for SFI.
2 All right. Starting with the security risk -- and this goes to the
3 question I was just asked -- we agree that all things being equal, a POSA
4 knew even more security would be obtained by encrypting the keys before
5 storing them. That's why the Tajima-Foster Ground 2 that I'll turn to shortly
6 is strong. And it's also why the Orsini Grounds and the other two IPRs are
7 strong.
8 But adding more security to the keys by encrypting them, as I
9 mentioned, is not required. SFI has other claims that both obfuscate and
10 further secure data chunks together. That's, for example, Claim 3 of the '854
11 patent. However, electing not to encrypt keys was still a known viable
12 option to a POSA, as I demonstrated with the evidence on Slide 12.
13 If you don't encrypt your keys, yes, there is a risk that when an
14 attacker gets all the encrypted data, they'll also have all the unencrypted
15 keys, and so it will be straightforward to recover the data. SFI's expert
16 admitted -- admits that on Slide 145. But when it's low-value data, that
17 might be a risk worth taking. It's a common trade-off in encryption between
18 complexity versus additional security that was not beyond a POSA's
19 capability to manage. We discussed that on page 29 of our reply.
20 But just because it was known that you could always add more
21 security doesn't make the equally well-known option of storing unencrypted
22 keys with data chunks, including obfuscated data chunks, any less obvious.
23 That's the In Re Fulton case we cited in our reply page at page 12, which
24 held that obviousness doesn't require the most desirable solution, as if I just
25 picked one of the known ways to store encryption keys and did so in a way

1 that produced no unexpected results.
2 On a related point, which I think goes to some of the questions I've
3 been asked, SFI's POR argues that the known approach of storing
4 unencrypted keys with data is potentially defeatable. You can see that in the
5 middle of the top left image on Slide 23. The security being potentially
6 defeatable doesn't extinguish obviousness. Again, an obvious modification
7 doesn't have to be the most desirable.
8 There's no such thing as perfect security. And Claim 1 doesn't
9 require some particular minimal level of security. As the Federal Circuit
10 said in the Intel v. Pact case, obviousness doesn't require the best solution,
11 only a suitable solution. The Court said that at 61 F.4th at 1380, which we
12 cite in our reply at page 12.
13 It is undisputed that storing Tajima's keys with the data chunks was
14 not only a suitable option, it had benefits over the alternative of storing the
15 key somewhere else. It's the simplified key management benefit that I
16 discussed back on Slide 15.
17 On the bottom left of the POR image on Slide 23, SFI argues that
18 encrypting the data fragments with another key before storing the fragment
19 would require additional key management. But in Ground 1 -- and there is
20 no other key, as I've mentioned before. SFI might be referring to Ground 2,
21 where we argued it would be obvious to encrypt the keys with another key.
22 But again, that's not our Ground 1. Ground 1 doesn't exclude
23 encrypted keys, again, but it doesn't require encrypted keys because the
24 claim doesn't require it. But even if SFI were trying to argue that there were
25 some additional key management required for Ground 1, that's wrong for the

1 reasons I've discussed before back on Slide 15, with support from Dr.
2 Bhattacharjee. So I'm -- that's all I have for obviousness of Ground 1.
3 And as I demonstrated, their arguments fail. So we also
4 demonstrated that Tajima anticipates because it has disclosure where the key
5 information is clearly referring to information that includes a key. But given
6 the number of topics I have to cover today, we're going to rest on our papers
7 for the anticipation ground for Ground 1.
8 And I'll move on now to Ground 2. Slide --
9 JUDGE KAZHDAN: Sorry. When you say you're resting on it,
10 are you giving up on it or you're just resting on your papers?
11 MR. NIEBERG: Just resting on our papers. We're not giving up
12 on it. We still contend and we think we demonstrated clearly that Tajima
13 does anticipate that the key information does include the key. But as I said,
14 we think the obviousness in this case is strong and there's such strong
15 corroborating evidence that it would at a minimum been obvious.
16 Slide 30. Ground 2 covers independent Claims 1 and 9 and the
17 dependent claims shown on Slide 30. So Ground 2 combines Tajima with
18 Foster, which I'll -- I will discuss now.
19 Slide 31 --
20 JUDGE GIANNETTI: Counsel, just a quick question. Why aren't
21 Claims 5 through 8 included in this ground? If they were obvious in light of
22 Tajima, why wouldn't they also be obvious in light of Tajima and Foster?
23 MR. NIEBERG: I think they would be obvious, but that's not part
24 of our ground. And so we didn't present that argument --
25 JUDGE GIANNETTI: Right.

1 MR. NIEBERG: -- of including Claims 5 through 8 in Ground 2.
2 JUDGE GIANNETTI: Okay. I just want to make sure that that's
3 your position, that they are in Ground 1 and not Ground 2.
4 MR. NIEBERG: I mean, yeah, we're not asking you to change the
5 claims and the grounds that we presented.
6 JUDGE GIANNETTI: All right. Thank you.
7 MR. NIEBERG: The arguments are the same, and they're
8 supported by the same. But the actual claims itself in Ground 1, those 5 to 8
9 are not in question.
10 JUDGE GIANNETTI: All right.
11 MR. NIEBERG: Okay. So Foster teaches storing encryption keys
12 with encrypted data chunks and further teaches to encrypt those keys with
13 another key, which is known in the art as a key encryption key. At
14 institution, Your Honors, has found a reasonable likelihood that this is
15 combination with the obvious. And the record post institution confirms that
16 initial decision.
17 The petition argued with evidence that it would have been obvious
18 to use a conventional key encryption key, like that taught in Foster to
19 encrypt the Tajima's keys. That was because a POSA would have known a
20 key encryption key would have added security to Tajima's system, which
21 we've touched on already.
22 As shown in the bottom left of Slide 31, SFI's own expert admits
23 that a key encryption key provides security because it prevents someone
24 with access to all the content from decrypting it. We agree with that. That
25 is precisely a motivation we identified for Ground 2. That's shown in the top

1 left of Slide 31 in the second highlighted portion. As a preview, again, that's
2 also the reason it would have been obvious to encrypt or seen these
3 encryption keys in the other two IPRs, which I'll discuss later.
4 Slide 32. On the right is evidence the petition cited to corroborate
5 that using a key encryption key to encrypt encrypted keys like Tajima's was
6 well-known in the prior art with well-known benefits. These references are
7 unambiguous in their teachings.
8 For example, Exhibit 1022 in the middle image on the right side of
9 Slide 32, we've highlighted where it says an encryption key should never
10 occur in clear form outside the cryptographic device. SFI does not dispute
11 the clear teachings in the prior art that encrypting encryption keys was well-
12 known. And it was -- and recommended by the prior art to add security to
13 encrypted data that is stored or transmitted outside the encryption device as
14 in Tajima.
15 So we made a strong showing in the petition that it would have
16 been obvious to store Tajima's keys with data chunks and encrypt those keys
17 with another encryption key, based on Foster and a POSA's background
18 knowledge of the benefits of encrypting keys with a key encryption key.
19 Slide 35 summarizes SFI's attack on Ground 2. It is just about the
20 motivation to combine Tajima and Foster. I'll address each of these in turn.
21 Slide 37. SFI argues there will be no motivation to encrypt the
22 Tajima's keys because the Tajima hides the keys by obfuscating them. SFI
23 says encrypting and obfuscating are redundant, by which SFI means
24 encrypting the keys and obfuscating them provides identical security
25 benefits.

1 SFI is incorrect. They provide distinct layers of security. So with
2 obfuscation, keys and data are stored on different storage devices. They're
3 swapped. And so that makes it harder for an attacker to obtain all the
4 encrypted pieces of data because they're on separate devices -- separate
5 storage devices and they're stored with a different key.
6 But that only works as long as an attacker does not obtain all of the
7 encrypted pieces of data. Alternatively -- or separately, encrypting the keys
8 with a key encryption key provides security even if an attacker gets all the
9 data chunks. The attacker would then still have to break the encryption
10 algorithm, which might be practically unbreakable, or they have to get their
11 hands on the key encryption key.
12 So using both obfuscation and a key encryption key is like having
13 a lock on your house door and an alarm system. SFI's argument is
14 essentially, well, if you already have a lock, why do you need an alarm? But
15 everyone knows why. The lock tries to prevent a thief from getting in. But
16 if they break the lock and they get in, the alarm will go off and provide some
17 additional security. They provide different security benefits for different --
18 JUDGE GIANNETTI: Counsel, is that a good analogy, though?
19 Are we talking about a lock and alarm or two different locks?
20 MR. NIEBERG: Well, you could call it two different locks.
21 JUDGE GIANNETTI: Yes.
22 MR. NIEBERG: But I think the reason I say -- I think that the lock
23 and the alarm are good analogy in that they're different forms of security.
24 And that's the point between obfuscation and key encryption key.
25 Obfuscation is -- its protection is store the pieces of data on different storage

1 devices and hope that an attacker can't get the data out of those storage
2 devices.
3 The key encryption key is different. It says even if the attacker
4 gets it, even if you have terrible storage devices that can go through data
5 chunks, the key encryption key will prevent them from decrypting the data.
6 So the --
7 JUDGE GIANNETTI: I see your point. Thank you.
8 MR. NIEBERG: Okay. Great. Thank you.
9 JUDGE BELISLE: Counsel, this is Judge Belisle. Where are you
10 keeping that key encryption key in your scenario?
11 MR. NIEBERG: So that's not required by the claim. But there are
12 conventional places where --
13 JUDGE BELISLE: Well, I mean -- but as far as you're saying it's
14 obvious, right, to have put these together.
15 MR NIEBERG: Yeah.
16 JUDGE BELISLE: So if it's obvious, where is it obvious to keep
17 that key encryption key to make this work?
18 MR. NIEBERG: Okay. So there were well-known key
19 management techniques for managing key encryption keys. The SSI patents
20 rely on conventional priority art key management techniques. And
21 essentially, it's just a higher security storage device kept in the system that
22 stores these key encryption keys with added security - the two -- because if
23 you want to prevent anyone from getting their hands on them.
24 For example, Tajima actually stores the data chunks and keys --
25 and key information on third-party storage devices out over the Internet. So

1 the person -- the entity that sent it out over there doesn't have control over
2 that. So there's a security risk that if those places are not so secure, an
3 attacker could get the data and the keys. And then with just obfuscation,
4 you're out of luck.
5 With a key encryption key, Tajima system encrypts those keys,
6 sends it to the storage devices so that even if someone breaks into those
7 storage devices and gets both the data chunks, you're okay because they still
8 need to get the key encryption key. Did that answer your question?
9 JUDGE BELISLE: In part. I mean, I'm still trying to figure out
10 why this would have been so obvious. Because it doesn't strike me that
11 managing that key encryption key, once all of those chunks have
12 fragments -- have their keys attached to them and then obfuscated that that's
13 a -- that seems to me like there's some complexity to managing the key
14 encryption keys, encrypting of those keys on those chunks for purposes of
15 decrypting them when you're pulling a variety of chunks from different
16 places.
17 That doesn't strike me as I'll just say easy, even within the
18 computer science world. So I'm just trying to get my head around why the
19 skilled artisan would have looked at Tajima -- and again, like I was kind of
20 saying earlier -- and let's assume that, yes, I mean, key encryption keys were
21 known and it's known what it does. So why would that skilled artisan have
22 said, oh, let's just do this?
23 And, like, that wouldn't add any layers of complexity or difficulty
24 or -- well, I'll leave it at that, you know, complexity or difficulty in the
25 obviousness world.

1 MR. NIEBERG: So we don't dispute that it is adding some
2 additional complexity. We do dispute that it's complexity that is beyond the
3 POSA's skill to manage. Because using key encryption keys are so well-
4 known -- decades in the prior art.
5 The problem with the complexity of managing a key encryption
6 key, it is -- was well-known. It wasn't a problem for a person of skill that
7 they couldn't address. It's just a trade-off. So it's a trade-off between some
8 additional complexity for some additional -- some, we would argue,
9 significant additional security.
10 So that's the balance of the -- a person of skill always makes in
11 security between convenience, complexity versus speed of recovery, and
12 how important is your data. And I'll note Foster, of course, is bringing the
13 key encryption key. So Foster is managing key encryption keys. Foster has
14 key encryption key. It has key management.
15 And so that just demonstrates that the management of key
16 encryption keys was a -- to the extent it was a -- to the extent there was
17 complexity to it, that complexity was well understood and manageable to a
18 POSA. It doesn't defeat obviousness because they knew that they could
19 manage the encryption keys. They knew their techniques for doing so.
20 They knew there were systems for doing so. And they knew their reasons
21 for the benefits of that additional cost of having to manage those keys.
22 Did that answer your question?
23 JUDGE BELISLE: In part. I mean, again, I come back to -- it's
24 because I keep hearing that, you know, key encryption keys, well-known,
25 everybody knew how to use them, everybody knew how to manage them.

1 But yet -- and despite -- yes, seemingly, more security is better than less
2 security. We have a reference like Tajima. And coming up in the program,
3 we have a reference like Orsini. But they didn't use it.
4 So for something that is supposedly so obvious and so easy, we
5 have two sets, Tajima and, like I said, Orsini at a minimum, where they
6 didn't do that despite all the greatness apparently in adding that extra
7 protection. So I'm just trying to understand if it is something that's so great
8 and so obvious, how is it we have references by folks in this business that
9 they didn't do it?
10 MR. NIEBERG: Sure. So one is they're just -- there are known
11 design alternatives. But the other answer is it depends in part on how
12 valuable your data is and what types of attack and attackers you're trying to
13 prevent against. So if you have low-value data, like personal information of,
14 like, an e-mail address, maybe it's not worth the extra cost and you're not too
15 concerned about having to do a key encryption key to protect it.
16 But if your data is personal banking information, well, then the
17 security benefits of a key encryption key -- the well-known key encryption
18 key is what a person of skill in the art would know. Well, in those cases, for
19 more valuable data or for the more determined attacker, there's a good
20 reason to add the key encryption key to get you that extra bit of security.
21 And again, it's just a trade-off. It's what attacks are you concerned
22 about for your data, how valuable is your data, how secure the storage
23 devices, et cetera. It's all just balancing trade-offs and selecting from, all
24 right, for this type of data in this situation, I want to take these well-known
25 encryption techniques.

1 And for this really important data -- well, I mean, there's always
2 some limit, but you're going to want to pick a lot of the well-known
3 encryption techniques because it's really important data. And so the key
4 encryption key is that additional security.
5 And I'll note too, Tajima doesn't say don't use a key encryption
6 key. And it's so well-known maybe Tajima said, of course people are going
7 to know it. I showed references that are a decade or more earlier that were
8 very clear in their teachings, you should use a key encryption key; do not
9 store your keys without encryption.
10 So, you know, I can't read Tajima's mind about why Tajima didn't
11 think about doing it. But a person, you know, in the art would have read
12 Tajima and said, you know, there's certainly a lot of situations where this
13 security has a flaw that no one disagrees with, that when you get all the data
14 chunks it's easy for an attacker to get it. And so how do -- what do I do in
15 those situations when I want to really want to protect my data? Oh, the
16 answer is easy, it's well-known, it's the key encryption key.
17 Have I now answered your question?
18 JUDGE BELISLE: I'm going to wait and hear how Patent Owner
19 likes your response.
20 MR. NIEBERG: Okay. And this relates -- so their argument on
21 the bottom left of Slide 37 says -- I think kind of what you were suggesting
22 is that it's very unlikely an attacker would get both of Tajima's data chunks,
23 so why bother doing a key encryption key.
24 Well, one, if you look to where they cite paragraphs 44 through 46,
25 those paragraphs say nothing about the likelihood of the storage devices

1 being breached. But more importantly, SFI doesn't dispute that it's possible
2 an attacker could get both data fragments. And just because something's
3 very unlikely, that doesn't mean you wouldn't want to protect against it.
4 Because as I just said, in some situations, your data is so valuable
5 you want to protect against even the most unlikely thing. It's unlikely any of
6 our homes are going to be broken into. But we still have a lock on our door
7 because the home is important. You want to put a lock on it, even if it's the
8 chance of anyone ever coming and breaking into any one individual's home
9 is very unlikely.
10 So if you turn to Slide 40, I'll address SFI's next argument. So
11 SFI's second argument alleges that Tajima and Foster are incompatible
12 because Foster has a desire for synchronization. And I'm going to talk more
13 about Foster synchronization shortly.
14 But basically, Foster wants to store and transmit each data chunk
15 with its key so the key and chunk arrive at a destination synchronously, at
16 the same time. That's because Foster's dealing with movie files, where
17 there's a benefit to being able to decrypt individual pieces and sometimes
18 you want the speed of being able to do that. But that concern does not exist
19 in Tajima.
20 On the right side of Slide 40, SFI's sur-reply recognizes that
21 Tajima's exemplary data set is media data, like a movie. And so that's where
22 Foster's synchronization benefits could possibly come into play. But SFI
23 also admits that those delays are not present and need not be avoided in
24 Tajima.
25 So we agree with that. Securing personal data -- when you're

1 securing personal data, synchronization in the sense that Foster used it is not
2 a concern. There's just two data chunks. It doesn't -- it's not like thousands
3 of data chunks in a movie file, so it's not that hard to swap them back. So it's
4 a red herring argument and does not defeat obviousness.
5 I'll move on to SFI's third argument, Slide 42. So SFI alleges that
6 Tajima and Foster are in different fields from each other. But SFI's not
7 alleging that Tajima or Foster are non-analogous art, testifies patent. And
8 there's no dispute that Tajima and Foster, therefore, are part of a POSA's
9 background knowledge. Also, they're not in different fields from each other.
10 They're both about securing data. So SFI's different fields argument also
11 fails.
12 Slide 43. So SFI's final attack on Ground 2 is that there's
13 allegedly no motivation to combine because Tajima doesn't disclose
14 attaching keys to data and Foster allegedly doesn't disclose data chunks. So
15 this argument fails because it ignores our combination. For the data chunks
16 limitation, Ground 2 relies on Tajima's data fragments, not Foster's data
17 chunks. And SFI doesn't dispute that Tajima's data fragments are data
18 chunks.
19 As for attaching keys to data fragments, that teaching comes from
20 Foster. And it was also obvious for the reasons I discussed in connection
21 with Ground 1. And so that's all I have on Ground 2. Unless Your Honors
22 have questions -- further questions, I'll turn now to the Foster-Hayhurst
23 Grounds.
24 Slide 45. So Foster-Hayhurst covers the claims of the '116 and
25 '854 patents that are shown on Slide 45.

1 Slide 46. The '116 patents claim one is shown again on the left
2 side of 46, that the disputes are the same for all claims covered by the
3 Foster-Hayhurst ground. On the right side of Slide 46 is Foster's Figure 8.
4 In orange, Foster has a data set, for example, a movie. The data set is split
5 into a plurality of payloads in green. Each payload is encrypted with its own
6 encryption key in blue. Those keys are encrypted by a key encryption key,
7 110, in red.
8 Then the encrypted key plus encrypted payload are stored
9 somewhere. I'll discuss the storage aspect shortly. So Claim 1 of the '116
10 patent requires separately storing the data chunks on a plurality of storage
11 devices. That's 1D in purple on the left. For that limitation, we combined
12 Foster with Hayhurst.
13 Slide 50. Hayhurst likes Foster's in the context of storing and
14 delivering chunks of digital content like a movie. Hayhurst stores the
15 chunks of a movie on multiple storage devices. In paragraph 8 of Hayhurst
16 in the bottom right, Hayhurst says this will provide a high level and a
17 deterrence to piracy. It's more secure because the data is now spread across
18 multiple storage devices rather than all located in just one or two places. It's
19 more than that.
20 But Hayhurst did not just provide security benefits. Hayhurst also
21 improves the way content is delivered to a destination. For example, when
22 you have multiple servers, multiple storage locations with a small piece of
23 data, that can avoid bottlenecks that occur when there's just one storage
24 location. So POSAs knew about the security and delivery benefits of
25 distributed storage like Hayhurst. Our petition has demonstrated

1 corroborating evidence of that on page 63 of our '116 petition and 62 of our
2 '854 petition.
3 Hayhurst also recognized that in a cable network, there's lots of
4 storage devices in people's homes. And so Hayhurst said we could leverage
5 that to use the storage devices in people's home to store the data for security
6 and also to shift some of the bandwidth away from the cable company to the
7 subscribers.
8 Slide 51. So the Foster-Hayhurst combination is straightforward.
9 It stores Foster encrypted data using Hayhurst distributed storage technique,
10 which is also used to deliver the data to a destination. A POSA would have
11 recognized multiple benefits from this combination.
12 As I just discussed on Slide 50, Hayhurst itself identifies some of
13 the benefits, like added security. And there were additional benefits that a
14 POSA would have recognized that we demonstrated with multiple pieces of
15 corroborating evidence, which is summarized on Slide 62.
16 But before I go there, I'd like to go to Slide 52. So Slide 52
17 summarizes SFI's three attacks on Foster-Hayhurst. I'll address each in turn,
18 beginning with the analogous art argument, Slide 56. Hayhurst is analogous
19 art at least because it's in the same field as SFI's patent, the field of securing
20 data. How do we know that? Hayhurst tells us that.
21 In the top right of Slide 56, Hayhurst says that its technical field
22 includes the secure handling and storage of data. SFI's table on the left of
23 Slide 56 from their POR -- and you're going to see on some of their slides or
24 at least one of their slides -- doesn't include that disclosure from Hayhurst.
25 It's important disclosure. And they probably didn't include it because it so

1 clearly reveals that Hayhurst itself says its field includes securing data.
2 But Hayhurst doesn't stop there. As shown in paragraph 8 on the
3 right side of Slide 56, Hayhurst recognizes and says its technique of
4 distributed storage provides a high level of security and increased deterrence
5 to piracy.
6 As Your Honor has correctly noted in the '116 institution decision
7 on page 23, Hayhurst's teachings and stated objective is a method to further
8 secure the data. So there should be no real dispute that Hayhurst's field
9 includes securing data.
10 So if you please turn to Slide 59. We also showed that Hayhurst is
11 analogous art because it addresses -- it's recently pertinent to at least one of
12 the problems identified in the patent. On the right side of Slide 59 are three
13 of the problems identified in SFI's patent that we demonstrated Hayhurst is
14 reasonably pertinent to.
15 SFI argues that the reasonably pertinent test -- what you have to do
16 is you have to check to see whether a problem in Hayhurst, the limited
17 bandwidth issue that Hayhurst addresses -- and see is that the same problem
18 and is that relevant to one of the problems in their patents, eliminating user
19 vulnerabilities. But that's not how the law on analogous art works. The
20 reasonably pertinent test asked whether the disclosure in Hayhurst -- not a
21 problem in Hayhurst -- is reasonably pertinent to any of the problems
22 addressed in the patent.
23 SFI does not dispute that Hayhurst is reasonably pertinent to
24 several problems discussed in their patents that we identified. And as shown
25 on the top right of Slide 59, we even showed how Hayhurst is relevant to the

1 only problem that SFI recognizes as a problem addressed by their patents,
2 user independent security. So Hayhurst's analogous art is both because it's
3 in the same field and reasonably pertinent to at least one and in fact several
4 problems in their patent. So SFI's non-analogous art argument failed.
5 I'll now move on to Slide 61 if there are no questions on analogous
6 art.
7 JUDGE REPKO: I have a quick question on analogous art. And is
8 it from your reply -- I think it's on page 3. Is it fair to characterize
9 Hayhurst's teachings as peer-to-peer file sharing?
10 MR. NIEBERG: No. Hayhurst discloses that you could use a
11 peer-to-peer, but it also doesn't require peer-to-peer. What Hayhurst --
12 actually, in the bottom that we relied on, there's a centralized server that
13 manages the different storage devices. Alternatively, it could be more of a
14 peer-to-peer.
15 The difference is that Hayhurst draws it's -- that there's no central
16 location kind of managing where it's -- so if you think, like, the Napster app
17 from years ago, it was all kind of -- the getting the chunks from different
18 places was kind of self-contained managed where the -- there was some -- it
19 wasn't centrally managed, where Hayhurst says you could do both or either.
20 But the one we relied on is there some central location that
21 manages where the chunks go and then how to send them to the pieces -- to
22 the destinations.
23 JUDGE REPKO: All right. And then you also say video
24 broadcasting. Is it fair to characterize Hayhurst in broadcasting? It seems
25 more like video-on-demand. And I guess Patent Owner is arguing that video

1 broadcasting, you know, is just kind of the opposite of Hayhurst.
2 MR. NIEBERG: Okay. So that's what I'm turning to now. I
3 could -- would -- should I ask you a question now? Would you like to see
4 where I'm going? I'm going to address that exact issue right now.
5 JUDGE REPKO: Yeah. No. But just on the analogous art aspect
6 of it, right? I mean, I think the way it's cited in the reply -- I guess I'm
7 looking at page 3 or something, you know -- saying the patent disclosures as
8 it applies to peer-to-peer and video broadcasting, two applications covered
9 by Hayhurst. So that's what I was wondering, is it a fair characterization of
10 that reference?
11 MR. NIEBERG: Of the Hayhurst reference?
12 JUDGE REPKO: Yeah.
13 MR. NIEBERG: Well, Hayhurst does teach techniques for how to
14 store and distribute digital content, in particular media content. But the
15 technique it teaches is the well-known technique of distributed storage. And
16 as Hayhurst says, that provides security. So Hayhurst is teaching a way to
17 securely store and deliver that data. So you could think of it as a genus
18 species. The genus of securing data is very broad. We argue that in our
19 reply, and that's why I didn't dispute it.
20 Hayhurst, at worst, is a species within that. It's a distributed
21 storage technique for securing data, and it talks about in the context of
22 movies. But it's still within that broader field of securing data.
23 JUDGE REPKO: Okay. Yeah. I guess it's Petitioner's Reply at 3,
24 it mentioned broadcasting. Is video broadcasting a fair characterization of
25 Hayhurst?

1 MR. NIEBERG: Well, I think video broadcasting is not a fair
2 characterization of Foster. And I think Hayhurst is primarily in the context
3 of distributing stored movies. And as I'm going to show now, Foster is also
4 about stored data, not live broadcasting.
5 JUDGE REPKO: I see. Yeah, that's kind of the understanding I
6 had when I looked at the Foster-Hayhurst. It seems like you're focused on
7 Foster's storage. That's why I was kind of curious to see, you know, that
8 mentioned in that footnote. But I don't know if the question was right. Feel
9 free to continue.
10 MR. NIEBERG: Yes. Well, for analogous art, we didn't have to
11 compare Hayhurst to Foster. We're comparing Hayhurst to the patent and its
12 field of securing data. So the reason they're compatible to combine is
13 because they're both in the context of storing digital media. But in terms of
14 the analogous art analysis, it didn't -- Hayhurst doesn't come into play, it's
15 just Foster and the patent.
16 JUDGE REPKO: Okay. Thank you.
17 MR. NIEBERG: Slide 61. So Hayhurst attack is going where we
18 were just discussing. They're saying there's no motivation to combine Foster
19 and Hayhurst.
20 So let's go to Slide 64, please. All right. So Slide 64 summarizes
21 the various benefits that would have motivated a POSA to make the Foster-
22 Hayhurst combination. We've cited multiple pieces of corroborating
23 evidence, and they fall -- some of them fall into multiple buckets about what
24 benefits would Hayhurst add to Foster: security, shifting bandwidth, faster
25 delivery of data.

1 And SFI doesn't dispute any of the benefits on Slide 64. In a
2 couple of places, which I'll address, they say there are some potential
3 drawbacks in security and speed. But they're wrong for that -- on those
4 issues. But even if they had some merit, balancing trade-offs and drawbacks
5 are always for obviousness. And in particular, in this field, there are
6 multiple undisputed benefits that would have -- in many situations, they
7 would have been reasons why POSA would have pursued the combination,
8 regardless of the alleged drawback.
9 So if we go to Slide 65. So SFI has four arguments on the
10 motivation to combine. And I'm going to start with arguments one and two
11 because these go to the question I was just asked, and they live -- they fall
12 together.
13 SFI argues that Foster is only about real-time streaming, by which
14 SFI means live television streaming. SFI argues that Hayhurst is
15 incompatible with live television. They're wrong about that, but it doesn't
16 matter because they're -- the main reason their argument fails is because
17 Foster is not limited to real-time streaming. So it doesn't matter if Hayhurst
18 were incompatible with live television.
19 We turn to Slide 66. So as I mentioned, SFI's first two attacks on
20 the motivation to combine, and really the heart of their attack on all of our
21 Foster ground, is that they're trying to limit Foster to live television
22 streaming. So in a moment, I'm going to show what Foster itself tells a
23 POSA how Foster is not limited to live television.
24 But before I do that, I think there's a really easy way for Your
25 Honors to reject all of SFI's live television streaming argument. And that's

1 because there's no dispute that Foster teaches to use the technique to protect
2 a movie. And we all know a movie is not created in real time. A movie
3 takes a long time to make. And then it's stored somewhere. It's usually
4 stored in lots of places.
5 And when a movie is shown, whether it's from a fixed storage
6 device like a DVD or downloaded from the Internet or even when it's shown
7 on a TV channel, the movie comes from storage. It's not made in real time.
8 So that's why Foster is at least relevant to systems that store movies and is
9 not limited to systems for viewing live TV, as SFI wants you to believe.
10 So again, for that reason alone, you can reject every argument SFI
11 makes that attacks the motivations to combine or modify Foster that we
12 advance in all three of our petitions.
13 JUDGE REPKO: So in your combination of Foster-Hayhurst, do
14 you need one key for all the chunks distributed to every subscriber, say, in
15 your movie scenario?
16 MR. NIEBERG: So in Foster-Hayhurst, there's two levels of keys.
17 There's the individual keys that encrypts each data chunk, and then there's a
18 key encryption key that encrypts that key. And so the data chunks get
19 spread across to the different users. And then when a user buys the movie or
20 clicks on the on-demand to have it sent to them, either streamed or
21 downloaded to them, then they will be given a key encryption key to decrypt
22 all the chunks that they get.
23 This gets really far down into the weeds. What actually happens is
24 there's this key management block that has the -- that is encrypted multiple
25 times with different key encryption keys. So it's like a key encryption key

1 for a key encryption key. And a user is given one of those things to unlock a
2 key encryption key.
3 JUDGE REPKO: So it's not the same one the other users get, you
4 know, the same duplicate key?
5 MR. NIEBERG: You don't have to. You could. It's a design
6 choice. You're sending the user that's authorized to use it. You send them
7 the key to unlock the movie. But of course, there's always the risk whenever
8 a movie's out into the world that someone could be nefarious and illegally
9 distribute and sell it.
10 And so in some systems, they'll have probably multiple
11 encryptions of the KEK and distribute it amongst multiple users. But it's a
12 design choice, a design detail for it.
13 JUDGE REPKO: But wouldn't that make it less secure if you're
14 distributing the same data to multiple users? Would it undermine Foster's
15 system at all by adopting Hayhurst's distributed system?
16 MR. NIEBERG: No. Because in Foster, the data still has to be
17 stored somewhere before it's sent to a user. So it's stored in one location in
18 Foster. In Hayhurst, it's stored amongst multiple locations so that it's harder
19 to actually get an attacker, an unauthorized user, to get the full data because
20 they have to go to, you know, 5, 10, 15, 20 storage locations. Where in
21 Foster, it's in one location.
22 And then when it gets to a user, in Foster it comes from that one
23 server. In Foster-Hayhurst, it comes from all the servers. So we disagree
24 that there's any loss of security in that context.
25 JUDGE REPKO: So I guess are you arguing that perhaps, like -- I

1 mean, if the data is distributed in chunks, then it might make it a little more
2 secure because the attacker might not have access to every single chunk in
3 the movie so that every little segment has less value than the entire thing.
4 But at the same time, you maybe lose some security because you may be
5 distributing the same key to every subscriber or that -- you're saying -- is that
6 like -- are you weighing this too? Is that your argument or is it --
7 MR. NIEBERG: Well, taking the steps, absolutely right that
8 distributed storage adds security, which is what Hayhurst teaches. It's what's
9 that SFI patent teaches. It was well-known. So there's no dispute there. So
10 there's a security benefit from distributed storage.
11 As far as the key, the key encryption key, in both Foster and
12 Foster-Hayhurst, the user only gets that key encryption key when they're
13 allowed to view the movie, right? You don't get movies for free. They want
14 to rent it to you. You want you to buy it. And when you buy it, that's when
15 they send you the key encryption key. So with Foster --
16 JUDGE REPKO: Right.
17 MR. NIEBERG: -- like, you get the movie, they give you the key.
18 So that one user has the key. In Foster-Hayhurst, it's only the users that have
19 been authorized, that have paid for that movie, that will have gotten the key
20 encryption key. And the same thing would happen in Foster, that the users
21 who bought the movie would get the key.
22 JUDGE REPKO: But there's multiple users, though, right? So
23 you're still -- you each have a copy of the same key?
24 MR. NIEBERG: No. Well, once authorized, then that's a design
25 choice. You could either give them all the same key or you can -- anytime a

1 movie is bought, you could swap in a new key. It's a well-known technique
2 of changing key encryption keys, which we demonstrated with evidence in
3 our reply.
4 JUDGE REPKO: Once you get authorized you're going to change
5 the key as well, possibly.
6 MR. NIEBERG: It's a design choice. Let's say it's a documentary
7 or it's a public movie, you don't care maybe that if everyone has that same
8 key. If it's something you want -- it's like a really valuable movie, it's a
9 preview, then -- like, it's a before release or for Oscar season when everyone
10 gets movies to view, maybe that case you're going to want to have multiple
11 encryptions of the key encryption key -- which is exactly what Foster does
12 and it still works in Hayhurst -- and you give them each of their own key
13 encryption key to get the key encryption key added, which is called the key
14 management block. It's just a bunch of encryptions of the key.
15 And just as further background, what -- you do that because then
16 you know if someone encrypts the data using -- if someone else encrypts it
17 with a key encryption key that doesn't belong to them, then you can tell who
18 was the nefarious actor or at least where the weakness was because their key
19 encryption key is now being used somewhere else.
20 JUDGE REPKO: I see. Is that all discussed in your reasons for
21 combining Foster and Hayhurst and the petition? Is there a specific part of
22 the petition you could point me to that specifically discusses how this key is
23 being distributed, or is this not necessary for your obviousness right now?
24 MR. NIEBERG: It's not necessary for obvious ground. Dr.
25 Bhattacharjee did discuss it in his -- well, it was discussed in reply in

1 response to SFI's arguments, both in our papers and in Dr. Bhattacharjee's
2 declaration.
3 In our petition, the changing of the key encryption key is not
4 required by the claims. It's just a further design detail that we didn't get into
5 the details of that. But Dr. Bhattacharjee explained that in Foster-Hayhurst,
6 as in Foster alone, the key would be held back until someone's authorized to
7 use it.
8 JUDGE REPKO: Thank you. I've no further questions on that.
9 MR. NIEBERG: Okay. All right. So as I mentioned, Foster's
10 about protecting a movie. So that's how you know it's not about real-time
11 TV. But Foster itself makes that clear. So Foster says prior art systems lack
12 synchronization. As I mentioned earlier, that means sending keys and
13 chunks separately. So they want to send asynchronously.
14 Foster wants to do it synchronously. So he wants a key in the data
15 to arrive at the same time so you can jump into a movie, let's say in the
16 middle, rather than have to wait until some later point. So Foster says --
17 talks about two categories of prior art systems, a digital rights management
18 system and a conditional access system. They're shown in Figures 1 and 2,
19 which are in the middle of Slide 66.
20 They're related systems. They're both about managing and
21 controlling a users' access to content. As Foster says and as POSA knew,
22 these systems were used to store content and deliver the stored content to a
23 destination. From Foster's paragraph 55 in the top left of Slide 66, Foster
24 says in a digital rights management system, content is packaged and loaded
25 onto a web server. That means in a DRMS, encrypted data is stored on the

1 server, and then it's delivered to a customer.
2 So SFI asks you to find that the DRMS, the digital rights and the
3 conditional access systems shown in Foster's Figures 1 and 2, are irrelevant
4 to and incompatible with Foster's encryption. And they want you to do that
5 because they know, and they have no dispute, that those systems were
6 storage based. So they're not only live TV streaming systems.
7 So if you go to Slide 67. So as shown in the top left of Slide 67,
8 SFI's POR admits that Foster is directed towards conditional access systems.
9 They admitted it. In our reply, we said, that's right, Foster is directed to a
10 conditional access system. And we demonstrated that a POSA knew that
11 conditional access systems included -- as I think came up before -- video-
12 on-demand systems where data is stored in encrypted form before delivered
13 to customers.
14 And that supports the exact motivation to combine because Foster
15 itself says in paragraph 2 -- sorry, Hayhurst says in paragraph 2 that
16 Hayhurst is helpful for a video-on-demand system, CR '854 petition at 59
17 and a '116 petition at 55. So for that reason alone, Foster and Hayhurst are
18 compatible because they're both recognized they could be used in video-on-
19 demand. Same applies --
20 JUDGE REPKO: So does Foster use the language video-on-
21 demand anywhere explicitly in the disclosure?
22 MR. NIEBERG: I believe on the DRMS Figure 1, it says an on-
23 demand server. I would have to look up again, I could be misremembering.
24 But in any event, our obviousness combination was that you would
25 implement Foster-Hayhurst -- the reason to combine Foster and Hayhurst

1 would be for video-on-demand purposes. You'd encrypt the data using
2 Foster's technique. And then you'd store and deliver the data using Hayhurst
3 technique, which Hayhurst explicitly says is useful for a video-on-demand
4 system.
5 JUDGE REPKO: So in your reply in page 7, you said paragraph
6 64, the e.g., video-on-demand, are you just referring to just generally storing
7 stuff? Or is there a specific application that would lead you to believe or
8 teach or suggest video-on-demand specific part of paragraph 64 of Foster.
9 MR. NIEBERG: So I want to get -- open Foster 64.
10 JUDGE REPKO: Yeah. I mean, I'm looking -- for example, 64
11 says, you know, they talk about type of content. They talk about video and
12 stream -- elementary content stream and parsing into units. More
13 specifically, are you thinking that the video-on-demand is in that?
14 MR. NIEBERG: What Foster says in 64, towards the bottom, is
15 indicated above, it's referring back to the DRMS and conditional access
16 systems. And so what Foster is trying to do is -- it says these prior art
17 systems, which are shown in Figure 1 and 2, which are -- would show a
18 server and a place where a data is stored.
19 Foster says those systems -- the prior art digital rights and
20 conditional access, they were missing the synchronization feature. The keys
21 and data arrive separately. So I'm going to improve those systems by
22 giving -- by including synchronization. And that allows random access to a
23 movie, like you jump into a movie in the middle.
24 JUDGE REPKO: Okay. So this still sounds a little bit like
25 streaming, though, right, with the delays -- you want to reduce the delays.

1 You're not downloading the entire content or downloading chunks of it.
2 You're sort of streaming -- you want to reduce the streaming delay. Am I
3 wrong about that?
4 MR. NIEBERG: Yeah, you are. But let me -- I could explain. So
5 it is beneficial for even when you download because you could -- if the
6 downloaded to -- if you have to wait for all the pieces to come when you
7 download it, you can't jump into the middle of the movie. But if the chunk
8 is stored with its own key, you could start getting the chunk from the middle
9 and not have to wait for the keys to come or from the key possibly stored
10 somewhere else that comes as a package together.
11 So even with pure downloading and even when you have
12 something stored on DVD, having the key and the data near each other helps
13 you -- makes it easier to jump into the middle of the movie, whether it's
14 stored or streamed.
15 JUDGE REPKO: So you're getting this video content, you know,
16 unencrypting it -- or decrypting it rather and were storing it in the decrypted
17 state or re-encrypting the old ones that you receive, in paragraph 64, when
18 you're talking about random access of content, right? Because you can think
19 of a scenario where you just -- you're downloading it and you're getting
20 these keys, you're decrypting, and then storing decrypted parts.
21 Hayhurst is talking about encrypting, like, parts of it. And then
22 you have parts that are stored in encrypted format, right? And you could
23 maybe do some random access to that unencrypted part. So 64, are you
24 envisioning a system here where it's unencrypted and stored at the end user?
25 MR. NIEBERG: No. The scenario is that the data will be

1 encrypted using Foster's techniques. So it's encrypted. Then those
2 encrypted chunks of Foster get put onto one or more -- to multiple storage
3 devices at Hayhurst in encrypted form.
4 Then when a user purchases the movie or downloads it or streams
5 it -- which I know you have a question about streaming -- they'll come from
6 the different Hayhurst storage devices in units of E-plus-chunk so that -- let's
7 say, for example, you want to jump to the movie in the middle, the
8 management system knows, all right, that you have to start at Chunk 158
9 that's stored on storage device N1198, get it from there, and then start
10 getting the rest of them. And so you could get -- you could start the movie
11 right in the middle by starting at the right chunk.
12 As to your streaming question, even in streaming, the data is stored
13 before it's streamed. And that's what Hayhurst can do as well. Streaming
14 just means that you can watch it as it's coming in. You usually also
15 download it. But as it's coming in, you could stream it. And it's just about
16 how fast the data is sent compared to how fast you need to decode it.
17 But in both cases, in our on-demand system, whether it's like an
18 iTunes, a server and a computer downloads it purely, or in a video-on-
19 demand like in a cable network where you can watch it as you're
20 downloading it, in both cases Hayhurst is the one that's storing the data and
21 then delivering it because it's coming from the different Hayhurst storage
22 devices. And it's coming in the -- it's encrypted when it gets to the user, and
23 then they decrypt it.
24 Does that answer your question?
25 JUDGE REPKO: Yeah. Well, I'm still looking at that paragraph

1 64, trying to make out that citation on reply 7 about video-on-demand. And
2 I think, I guess, it's probably you're focused on that last sentence, you know,
3 about DRMS and CAS. And to me, it does look like it's saying the packet's
4 transmitted, it's packaged with the title key that's it encrypted. The recipient
5 can access and decrypt that content stream at any packet.
6 So I mean, it does seem like it's a little different than Hayhurst, but
7 maybe that doesn't matter because it's a combination. It seems like it's
8 maybe using Hayhurst primarily for the storage aspect.
9 MR. NIEBERG: Well, I think it's both. As far as the combination
10 goes, it doesn't matter for the reason you just mentioned because we're
11 putting this combination into a video-on-demand system. A little of the
12 confusion for the stream, that terminology, it's called a content stream.
13 That's just how it's phrased.
14 For example, in the MPEG standard, they call it a content stream.
15 But MPEG stream could be stored on a DVD. It's still called the elementary
16 content stream, even though it's not streaming. It's just a terminology used
17 to describe that data set, but it's not actually limited to streaming. It's called
18 the content stream, maybe because it's a movie and a lot of images coming.
19 I don't know the historical reasons for that. But it's not limited to streaming,
20 if that answers your question.
21 JUDGE REPKO: Yeah. I mean, I think in the petition you also
22 said, well, the content units are individually accessible and agnostic to where
23 and how they are stored compared to the other content units. So in this way,
24 I get -- you're saying it's similar to Hayhurst's subscriber storage devices. Is
25 the 64 -- does that seem to be consistent with 64 as well in page -- of

1 paragraph 64 of Foster?
2 MR. NIEBERG: Yes. Because Foster is, as we explained in our
3 reply -- so and our combination was about on-demand. They're both -- it's
4 known for on-demand. In our reply, we're pointing out that Foster tells a
5 POSA that it's compatible with on-demand for the reason we had our
6 petition. But further because when Foster -- you read Foster context in 64, it
7 talks about DRMS and conditional access systems. And we cited a wealth
8 of evidence that's undisputed, that both of those systems were used for
9 storage-based delivery of content.
10 So what Foster does is Foster treats the conditional access system.
11 He's thinking of that like a cable on-demand system where you're getting it
12 from a cable system. And the digital rights management on-demand is more
13 like an iTunes, server-to-computer type system. They're both -- for purposes
14 of our combination, they're not that different. They're no different because
15 there's still a server storing it and then delivering it.
16 So Hayhurst could do both, it's either storing it in a cable network
17 or storing it in a -- on a website. And that's why the -- we're using the
18 broader term on-demand rather than cable video-on-demand versus iTunes
19 purchase-on-demand type of system.
20 JUDGE REPKO: Right. And I guess the relevant part seems to be
21 like what you're encrypting and when. And it doesn't seem like -- if you
22 look at 64, the idea is that the receiver is going to store the encrypted
23 contents and it's going to have everything it's needed to decrypt that content.
24 Whereas it's a little different than the Hayhurst where you have everything
25 distributed and you're kind of passing around different chunks and stuff.

1 And I guess in your combination, it seems like you're kind of
2 replacing some of that functionality in 64 -- in paragraph 64 with that
3 Hayhurst storage aspect.
4 MR. NIEBERG: Okay. So I think I understand now. What we're
5 saying is even in Foster, the storage that's referred to in 64, that's talking
6 about at the user after they bought the movie. But before they get the movie,
7 it's stored somewhere, right? It has to be stored somewhere. It's not made in
8 real time.
9 And so Foster has -- tells you in a DRMS and a conditional access,
10 there's some -- as a POSA knew, there's some server storage. It delivers it
11 point-to-point, server to person. So when it's talking about the recipient
12 storing it, when that recipient's an end user, it's just one storage device that
13 stores it at the end.
14 In Hayhurst, you replace Foster's one storage server with multiple
15 servers. And then when a user buys it in Foster-Hayhurst, that data comes
16 from all those servers. And that's the storage that 64 is referring to. It's after
17 it's delivered to a user, it's stored at the user collectively. Before, it's stored
18 in bits and pieces everywhere in Foster-Hayhurst, and then it's delivered all
19 to one user that stores it.
20 JUDGE REPKO: Mm-hmm. Thank you. I have no further
21 questions on that. You may proceed.
22 MR. NIEBERG: Slide 72. And just to reinforce that Foster is
23 compatible with a digital rights management system and which there's no
24 dispute is heavily -- it was well-known, and we demonstrated with evidence
25 used for storage-based video-on-demand type systems. This is Foster's

1 cover. The cover of Foster's Figure 1, that's the DRMS system. And SFI
2 would have you believe that Foster is irrelevant to DRMS, even though
3 Foster puts that on its cover. So I don't think that is consistent with what
4 usually the figure on the cover is representing.
5 Slide 77. So here's, as I mentioned, all of the evidence we cited
6 both in our petitions and reply about corroborating with clear evidence that
7 conditional access systems and DRMS systems were well-known and used
8 in the prior art for storage-based techniques for the video on -- we use video-
9 on-demand. I mean, the easiest to understand. But they're well-known for
10 use in conditional -- for video-on-demand type systems where one or more
11 servers store the encrypted data and then deliver it to a user which can
12 stream or download it -- or stream and download it from the server or
13 servers.
14 And so for this reason -- this is why SFI attacks on the Foster-
15 Hayhurst Ground and Foster alone are incorrect, that Foster is limited to live
16 streaming. I just want to emphasize, again, Foster is about a movie. And a
17 movie is not live. It has to be stored somewhere. And then it has to be
18 delivered to a user. And we're saying in the Foster-Hayhurst combination
19 that storage and delivery leverages the benefits that Foster -- Hayhurst
20 identified: the security, speed, intelligence, et cetera.
21 Slide 80. Just very briefly on Slide 80, this argument is -- their
22 second argument about Hayhurst being incompatible with live TV, it's not --
23 and Dr. Bhattacharjee explained that and cited evidence. But it doesn't
24 matter because Foster is not limited to live television streaming.
25 Slide 82. So SFI's third attack on the combination alleges that

1 Hayhurst would make Foster slower. That's incorrect. On the right side of
2 Slide 82 are several pieces of corroborating evidence we cited that shows
3 that POSAs knew -- Hayhurst says that the POSA also knew that a
4 distributed storage system actually makes delivery faster. It does that
5 because the data chunk is stored on multiple devices.
6 And so if one device is not working, you can get it from another
7 one or a closer one rather than the potential bottlenecks of a point-to-point
8 type delivery system that Foster is just -- it's compatible with other types, but
9 it only gives the examples of a single server delivering the data to a user.
10 As I've mentioned already, when -- whether you download or
11 stream a movie, the source of that movie is a storage device. It's not made in
12 real time. Foster is not about -- and certainly not limited to -- real-time
13 streaming.
14 Slide 84. So SFI's fourth and final attack on the motivation to
15 combine is the -- is an allegation that Hayhurst would somehow make Foster
16 less secure. Your Honors correctly made a preliminary finding in your
17 institution decisions that Hayhurst add security to data. That's on '116 Paper
18 11 at 23; and the '854 Paper 15 at 9.
19 And so as I discussed back in the analogous art section on Slide 56,
20 Hayhurst explicitly says that its technique adds security and deterrence to
21 piracy because it doesn't store all the data in one place. A POSA would
22 agree.
23 On the top right of Slide 84, SFI's expert admitted that breaking up
24 data and storing it in different locations can provide a security benefit
25 compared to storing it in one location. Their own patents say this. And they

1 don't allege to have invented the idea of distributed storage. And if they did
2 allege that, we've shown multiple pieces of corroborating evidence that that
3 was well-known long before SFI came along.
4 But even if some aspect of Hayhurst made some aspect of Foster
5 less secure -- and we do not agree -- that's an attack on the references
6 individually. And at worst, it's just a potential design trade-off, an alleged
7 reduction in security, balanced against all of the undisputed benefits of
8 Foster-Hayhurst compared to Foster alone that we identified: speed, the
9 security of distributed storage, intelligent delivery of content, et cetera. And
10 managing those trade-offs was not beyond a POSA's capability. And so it
11 does not defeat obviousness.
12 Slide 87. So this, I think, goes to a question I was asked a short
13 while ago. And it's a good question, it's important. So as part of SFI
14 security argument, SFI alleged that Foster wants to be able to change the key
15 encryption key. But allegedly, Foster would not make that -- would make
16 that harder or -- will make it harder. I don't think they even alleged
17 impossible, they just say harder.
18 Our replies explained why that's wrong. So first, we identified
19 where Foster makes clear that changing the key encryption key is optional.
20 It's not required, it's optional with Foster. That's discussed in Foster's
21 paragraph 54, which our '116 reply cited at pages 27 through 28 and
22 discussed, and our '854 reply said that at page 11. And Foster's paragraph 54
23 is on Slide 85, if you're interested in looking at that.
24 But our replies went further. And what we demonstrated is that
25 even if a POSA wanted to change the key encryption key in the Foster-

1 Hayhurst combination, we cited multiple pieces of corroborating evidence,
2 like 1079 and 1080 shown here on Slide 87, that teach -- that it was known
3 that changing a key encryption key in a distributed system like Foster-
4 Hayhurst was known.
5 SFI's sur-reply on the bottom left alleges that these references only
6 teach changing other keys, not a key encryption key. That's incorrect. I've
7 underlined here on Slide 87 where these references also keep changing the
8 key encryption key.
9 JUDGE KAZHDAN: Just so you know, you've been on for 1 hour
10 and 20. You still have time, but I just want to give you a heads up on where
11 you are in your time.
12 MR. NIEBERG: Oh, thank you very much. And so I think SFI's
13 fourth argument is really just a flavor of its live TV argument. Because for
14 stored movies, you have more time to change things like a key encryption
15 key. You don't have to do it immediately. So SFI's fourth and final attack
16 on the motivation to combine fails along with SFI's other three arguments.
17 Just very briefly on Slide 91, SFI's sur-reply alleges that we
18 changed in our replies from Hayhurst storage context to Foster storage
19 context. And that's not true. Our combination has always been storing
20 Foster encrypted data using Hayhurst delivery and -- storage and delivery
21 technique. All we did is demonstrate why they're incorrect to narrow Foster
22 to live television.
23 But we didn't switch to Foster storage context. It's always been
24 Foster is compatible with storage techniques. And in our combination, it's
25 used in a storage-based system, which Hayhurst clearly is compatible with.

1 It's all about storage and an on-demand. So we did not make any new
2 contentions. We didn't make -- change our combination. It's always been
3 the same.
4 And so now, I'm going to turn briefly to the last topic for Foster-
5 Hayhurst, and that's on Slide 94. So SFI alleges for -- in all three matters
6 that Foster does not teach data chunks. But as you can see in the top left of
7 Slide 94, SFI's own expert admitted that the share or the data chunk, it's just
8 the thing that something gets split into. And that's what happens in Foster.
9 So on the right side of Slide 94, Foster has that data set in orange.
10 It's one large block of movie. You can see there's no divisions in it, just a
11 large block of a movie file. It gets split into green pieces, which Foster calls
12 payloads. And then each payload is put into a content unit.
13 And Foster's paragraph 64 on the left even says that the data is
14 parceled into content units, its split. So it needs exactly what the plain
15 language requires. It needs exactly what SFI's expert said in the shares the
16 chunks require.
17 Slide 95, very briefly, SFI makes this big deal about how their
18 patent talks about a packet could be divided into chunks. And they cite
19 some literature that says a packet could be divided into chunks.
20 As a first principle, black-letter law, it doesn't matter what Foster
21 says -- and they say that Foster doesn't call its data a chunk, it calls it a
22 packet at times. It doesn't matter what Foster calls it. What matters is
23 whether Foster's payloads meet the claims. And they do for the reasons I
24 just mentioned.
25 But in addition to the extent that the literature, whether they call it

1 the packets and chunks, we cited multiple pieces of corroborating evidence,
2 one of which is shown on the bottom right of Slide 95, Exhibit 1082. And it
3 expressly says that each packet is a chunk of a particular elementary stream.
4 It's even in the exact same context of Foster, the preferred
5 embodiment of an MPEG stream. It calls it a chunk. Each packet is a
6 chunk. So SFI's argument, trying to distinguish between packets and
7 chunks, fails.
8 And on Slide 96, you'll see additional corroborating evidence that
9 we cited that also refers to packets as a chunk of a data, chunk of a data set.
10 If you go to slide -- so I think that's all I have now because I'm
11 running short on time for the Foster-Hayhurst Grounds. I'm going to switch
12 now to the Foster ground for the '609 patent on Slide 110.
13 All right. So we've talked about Foster a few times. Foster's about
14 encrypting a digital content, like a movie. As shown in Figure 16 on the
15 right side of Slide 110 in orange, there's a content owner, like a movie
16 studio. The content owner sends the movie to what Foster calls a content
17 service provider, like a cable company or an iTunes-like website.
18 As Foster says in paragraph 39, the content service provider is the
19 pipeline through which content gets from the content owner to the customer.
20 So the content service provider at Figure 16 is the entity in the middle
21 between the content owner and the end user.
22 So Claim 1 also recites some hardware elements. As shown in the
23 top left of Slide 110, Foster's limitation 1A requires a processor. Foster has
24 a processor. There's no dispute, that's in yellow on the right side of Slide
25 110. And then Claim 1 requires the processor to execute code to implement

1 the method -- steps.
2 Foster's paragraph 78 shown in the middle of Slide 110 discloses
3 that Foster's method is implemented by executing a computer program,
4 which SFI does not dispute is code executed by Foster's processor. So
5 limitation 1F recites another hardware element. It requires the memory of a
6 storage device that is coupled to the processor to store at least one data
7 chunk.
8 So in Figure 16, we illustrated one example of where Foster's
9 processor is coupled to a storage device. Now, the processor goes over a
10 Bus 410 to a memory, which is a storage device. And then if the -- then if it
11 wants to send it to a user or a customer or another content service provider,
12 the transmission system and Foster's - and the content service provider will
13 send it over some link -- in the top right, in green -- to that storage device,
14 over the Internet or it could be a local area network. Foster is broad in that
15 sense.
16 JUDGE BELISLE: Okay. Counsel, this is Judge Belisle. Let's
17 focus on this because this is a point of contention here.
18 In your petition, it identified 430 as the claimed, at least one
19 storage device. How is it that the CPU in a separate computer system
20 executes code that causes item 430 to store data? So how does this
21 computer over here execute a code that causes a different device in
22 somebody's home to store data?
23 MR. NIEBERG: Okay. I'm glad you raised that question. So we
24 had an obviousness and an anticipation argument. So all of the attacks about
25 instructions to store are about the anticipation argument. And I was

1 actually -- I wanted to focus on the obviousness argument. Because in that
2 case, SFI has no argument that the processor is not instructing the storage
3 device to store.
4 Because in our obviousness argument, we allege that Foster had
5 reason to store content in the Memory 402, not just the recipient storage
6 device. We allege for our obviousness argument that the processor would
7 store the content in the Memory 402, which Foster says can include
8 traditional conventional storage devices. So in our obviousness argument --
9 JUDGE BELISLE: So let's stop there. Are you no longer
10 arguing that CPU 406 executes code that stores data on Storage Device 430?
11 MR. NIEBERG: No. We are still arguing that. So --
12 JUDGE BELISLE: Okay. So then explain to me how that does it.
13 MR. NIEBERG: Okay. So first, that requires what we think is a
14 new claim construction by SFI that they didn't present pre-institution, that
15 there must be some instruction from the processor to store. And --
16 JUDGE BELISLE: Well, it says right there, executing code in the
17 claim. That's why I'm trying to -- I don't see with the claim construction
18 argument. Execute code on the processor to store that data on the storage
19 device, how does it do that? How is it possible it can control that storage
20 device?
21 MR. NIEBERG: Well, control, I don't --
22 JUDGE BELISLE: Based on the disclosure or the reference.
23 MR. NIEBERG: Well, I think you also have to read the claim
24 language in light of their specification.
25 JUDGE BELISLE: Mm-hmm.

1 MR. NIEBERG: And then their specification, there's no
2 discussion at all about code and the processor sending instructions. What
3 their patent discusses is having remote storage devices, devices out over a
4 network that have their own processors, have their own CPUs. And yet
5 somehow, those storage devices -- that's the only written description support
6 they have on this claim.
7 They still -- if there is written description support, which we could
8 assume for purposes of these matters, those remote sometimes third-party
9 storage devices are storing data. So that's why in our view, the claims don't
10 require the processor to instruct the storage device to do it because their
11 patent has no support for that. Their claim language has no support to
12 construct the storage device to do it.
13 But to your point, let's assume Your Honors agreed with that
14 construction. There's two points that I want to make clear. One is for our
15 obviousness argument; there's no dispute that Foster's processor is
16 instructing its local memory storage device to store. And we've made
17 several arguments why that would have been obvious.
18 And then under their construction, if you look to their infringement
19 contentions, if you look to the patent, if you look to pre-institution, they said
20 nothing about this construction argument. They could have made it pre-
21 institution, and Your Honors maybe would have found it valid and maybe
22 you would have thought, oh, maybe we're not going to deny institution, and
23 we wouldn't have an estoppel. But now, they sandbagged us. They waited
24 to post-institution. They said now the claims have to --
25 JUDGE BELISLE: Counsel, they're not even required to file a

1 preliminary response. So I don't want to hear all of this. I just want to hear
2 the response to my question as to how Foster shows executing code that
3 stores the data on item 430. There's either an argument that it does or it
4 doesn't.
5 MR. NIEBERG: So Foster executes code in that embodiment,
6 where the 430 is a remote recipient that processes the data, sends the data, is
7 holding it, and then it's downloaded to that unit. And so the processor's code
8 is what it's executing. It's packaging it and preparing it for storage on the
9 storage device.
10 Does it instruct the storage device to store? It depends on the
11 implementation detail and what embodiment. And so in our obviousness
12 argument, the processor is storing, for its own purposes, at a local storage
13 device. In our anticipation argument in the petition, it was storing it at a
14 recipient, which we believe, and still do, meets the plain language of the
15 claim.
16 And then we explained, well, if you -- if SFI's right that the claim
17 requires instructing it, we presented multiple obviousness arguments
18 separate from our petition's obviousness argument, just on their claim
19 construction, that also renders it obvious. Ultimately, for the same reason
20 it's obvious under our -- in our petition. The same argument is that the
21 processor would store it at a storage device directly coupled to it -- of the
22 Memory 402.
23 JUDGE BELISLE: So let's just stick on that since we seem to
24 keep drifting towards obviousness and the internal memory. Where in a
25 petition does it rely on the internal memory as the storage device?

1 MR. NIEBERG: Yes, Your Honor. So in our obviousness --
2 JUDGE GIANNETTI: Counsel, I just -- I want you to answer this
3 question and continue with this with Judge Belisle. But I just wanted to
4 remind you that you are in your rebuttal period.
5 MR. NIEBERG: Yeah, thank you. But I do think these are
6 important points to make.
7 JUDGE GIANNETTI: I agree.
8 MR. NIEBERG: So we allege -- and I'm sorry, I'm just searching
9 for it right now. I don't have it at my fingertips. So in our Foster ground --
10 give me one moment please. So on page 74 into page 75, so we argued that
11 for obviousness that, as illustrated in Figure 16, the -- I'm sorry, I'm looking
12 at the wrong page. I apologize.
13 So bottom of 76, so we argue that POSA had reason to store
14 Foster's encrypted content in the memory of storage devices coupled to the
15 processor through a bus, direct wired, or wireless connection or network-
16 based interface. As discussed above, Foster's system 400 is or can be part of
17 a content service provider.
18 As illustrated in Figure 13, Foster's system 400 includes Memory
19 402, which comprise any known type of data storage, including one or more
20 type of data storage distributed across plural physical streams. And then
21 continued, Foster's Memory 402 is coupled to CPU 406 via Bus 410, and
22 that includes storage devices.
23 And then we explain reasons why a POSA would have reason to
24 store it in the Memory 402, which there's no dispute is receiving instructions
25 to store from the processor. Does that --

1 JUDGE BELISLE: Do you have any other statements in the
2 petition that you'd like to rely on for where the argument was made?
3 MR. NIEBERG: Well, we could --
4 JUDGE BELISLE: Where the chunks are stored on that internal
5 memory? I mean, the internal memory is obviously used to store stuff. And
6 it is a memory and it is going to be a storage device. But from my reading of
7 the disclosure, it discusses storing all of those items that are numbered in
8 Figure 16.
9 What I don't see is any disclosure -- or at least none that's been
10 pointed out to me -- in the reference that shows that the memory is storing
11 those chunks, the content, the data chunks.
12 MR. NIEBERG: Okay. Two points to make there. One, the claim
13 is only required storing at least one data chunk. It doesn't require storing all
14 of them. So as you said, the memory is clearly going to store at least one of
15 the data chunks as --
16 JUDGE BELISLE: Well, let's -- I didn't -- I did not say that.
17 MR. NIEBERG: Okay. I apologize. But we did argue that in our
18 reply. But to your broader point, Foster says that Memory 402, it can
19 actually include more than just like RAM. I think that's what you're thinking
20 of, like a local RAM. But it says -- and we quoted it and pointed out that
21 402 can comprise any known type of storage device, data storage device,
22 including traditional storage devices that the processor pushes the data to, to
23 store it for purposes of downloading it when required.
24 And we argued that in our obviousness combination. Beyond what
25 Foster itself discloses, a POSA would have had motivation to take Foster's

1 system, put it in a video-on-demand system. So like an iTunes, they would
2 encrypt the data using Foster's technique, and then that same processor
3 would store that data for on-demand uses that we've discussed before. That
4 was our obviousness argument.
5 JUDGE BELISLE: Okay. Well, I'm not going to eat up more of
6 your time. I think we can -- we'll probably be coming back to this on
7 rebuttal.
8 MR. NIEBERG: Okay. So very briefly, I want to discuss the
9 Orsini grounds. And if you turn briefly to Slide 134. So for the Orsini
10 grounds, the only disputed limitation is a limitation shown here. And it
11 requires performing an encryption operation based on the external key that
12 draws the plurality of data chunks.
13 And our petition made several anticipation and obvious arguments.
14 Your Honors were not yet persuaded by them. And to simplify it, we -- and
15 our replies focused on the obviousness argument. That is what we discussed
16 earlier for Tajima-Foster, which is encrypting or seeding these keys with a
17 conventional well-known key encryption key.
18 And so if you turn to --
19 JUDGE REPKO: So are you abandoning those other grounds or
20 conceding them?
21 MR. NIEBERG: No, Your Honor. We still think they're valid.
22 But to simplify the issues for dispute, we wanted to focus on the argument
23 that we thought -- that we think is not only very strong, but SFI's response is
24 very weak. And so we focused on that. And it's also very similar to the
25 argument in the '116 patent, Tajima-Foster, where the use of a key

1 encryption key was well-known and had well-known security benefits.
2 And just as a brief reminder or just to reiterate, so if you turn to
3 Slide 140, here are the two pieces of corroborating evidence we had in our
4 petitions that we quoted and cited. There's no question there in our petitions.
5 And they were very clear in their teachings. Exhibit 1036 and the top right
6 of Slide 140 taught that when you store -- when you transmit and store data
7 chunks with keys, as in Orsini, the security comes from encrypting the keys
8 with a key encryption key. It's a very clear teaching and motivation to do
9 that in Orsini.
10 Exhibit 1035, bottom right of Slide 140, it went -- it even taught
11 that a POSA that encrypts key -- that encryption keys should never occur in
12 clear form outside the cryptographic device. But that's what Orsini does.
13 And its reason we discussed before as it's on -- you could do it. You don't
14 have to encrypt them, or maybe for simplicity you wouldn't.
15 But a POSA knew that if you have important data and you're -- you
16 have a really motivated attacker, you're going to want to use a key
17 encryption key to encrypt Orsini's keys. And that is the only distinction that
18 SFI alleges between their patents and Orsini.
19 And SFI does not allege that they invented a key encryption key.
20 They do not allege that they invented the idea of using a key encryption key.
21 By definition, it encrypts keys. They don't allege that there are any
22 unexpected results. They just selected this one over -- the delta from Orsini
23 is just using the well-known conventional key encryption key for its well-
24 known conventional benefits that our petition documented with multiple
25 pieces of corroborating evidence.

1 JUDGE REPKO: So going back to that -- I don't want to rehash
2 the whole discussion about Philips v. Google. You did mention that in
3 another page. But I think with respect to pages 43 and 44 of the petition, I
4 mean, did you explain how you're modifying Orsini and why you would do
5 it? Or, you know, that 1035 reference, the Ehrsam, is it -- are you saying
6 that there's a missing limitation and you would supply the limitation through
7 Ehrsam and it was obvious to do that, or just simply that it was possible to
8 do that?
9 MR. NIEBERG: Our argument is that there is no missing
10 limitation here. It was well-known in the prior art. So about missing it --
11 just the missing limitation analysis of Arendi and DSS doesn't come into
12 play. As you're -- but I think what you're asking is whether that's taught in
13 Orsini. So we had anticipation arguments that we did and we still believe
14 teaches techniques that meet the claim. Orsini, however, does not teach
15 using a key encryption key to encrypt the share keys.
16 So if you go back to Slide --
17 JUDGE REPKO: I guess my focus is on your explanation on
18 pages 43 and 44 related to the Exhibit 1035.
19 MR. NIEBERG: I'm sorry, which petition are you looking at? I
20 just want to make sure I'm --
21 JUDGE REPKO: It is for 15 -- or 215 case.
22 MR. NIEBERG: 215 case. So we cited -- we demonstrated that
23 Orsini does not encrypt the shared keys. And we cited two pieces of
24 corroborating evidence that taught a POSA you shouldn't do that. There's a
25 security risk there.

1 And so, you know, as I showed you, they were extremely clear in
2 their teachings as that the security in situations like Orsini, when data is
3 stored with keys is the -- you should encrypt them. That's what those
4 teachings are. And so that was the motivation. The person skilled in the art
5 knew of this background knowledge that when you have -- when you're
6 storing keys with data and the keys are unencrypted, yeah, you could do that.
7 But if it's really important data -- and in most cases, you don't want
8 to do that. You're going to want to encrypt them because there's a security
9 risk. And those teachings in our -- in the petition were very clear. And in
10 response to their reply, challenging whether it was -- that is a missing
11 limitation and that there would be no motivation. We didn't make a new
12 meaningful contention. We continued with the same contention.
13 There would be motivation to do it because it was well-known. It
14 provided security benefits. And those security benefits are, for example,
15 that -- when an attacker gets all the data chunks, Orsini's obfuscation falls
16 apart then, but the key encryption key continues to provide security even
17 when a person -- even when an attacker has all the data chunks. And that's
18 exactly why it was so pervasive in the prior art to use the key encryption key
19 to encrypt keys. That's what it's for. It's why it existed.
20 Yeah. And so on page 43, for example, of our -- the 215 matter,
21 we said -- I think if you're looking at that, a POSA had reason to encrypt
22 Orsini's keys with a KEK, a key encryption key. And we cited Exhibits
23 1035 and 1036 as evidence that a POSA had that motivation. And we even
24 quoted their clear teachings to do it.
25 JUDGE REPKO: A POSA had that motivation, it sounds like, you

1 know, you're modifying Orsini in a way, the -- you're not using them to
2 show something that Orsini already teaches.
3 MR. NIEBERG: For obviousness, we -- that's correct. We were
4 using those references. It's very similar to -- you mentioned the Philips,
5 Google, and the Tajima Ground 1, is that we were using the well-known use
6 of key encryption keys that we corroborated with multiple pieces of prior art
7 as a POSA's background knowledge. And we use that background
8 knowledge as the motivation to add to Orsini the encryption of those keys.
9 Orsini encrypts other keys. But if -- it doesn't say to encrypt those
10 shared keys. And our motivation was, well, a person skilled in the art knows
11 that's not the better security in most cases, especially when it's more
12 important data. And that's why the evidence in the art is clear, you should
13 encrypt encryption keys. And that's what we added, that background
14 knowledge to -- as modification
15 So single reference obviousness. Because it was so pervasive, we
16 cited two. And in our reply, we cited three or four more. Because it's just so
17 well-known that the knowledge, the desire, and the teaching to use a key
18 encryption key to encrypt keys, like Orsini's that are unencrypted but sent
19 somewhere else, which is dangerous.
20 JUDGE REPKO: Mm-hmm. I don't have further questions.
21 MR. NIEBERG: And with that, I will reserve the remainder of
22 my time for rebuttal.
23 JUDGE GIANNETTI: All right. Thank you.
24 JUDGE KAZHDAN: Just to let you know, you have about 15
25 minutes for rebuttal.

1 MR. NIEBERG: Okay. Thank you.
2 JUDGE GIANNETTI: All right. And with that, let's take a 10-
3 minute break. And we'll be back -- I guess, it would be 3:05. All right.
4 3:05, let's come back in 10 minutes. Thank you.
5 (Whereupon, the above-entitled matter went off the record at
6 3:05 p.m. and resumed at 3:15 p.m.)
7 JUDGE GIANNETTI: Okay. So we're back on the record. And
8 we're going to now hear from the Patent Owner who is -- who's making a
9 presentation for the Patent Owner? Who's leading off?
10 MR. LOWENSTEIN: Good afternoon, Your Honors. This is
11 Nathan Lowenstein for Security First. I'm going to start the discussion
12 before turning the microphone to Mr. Iancu and then Ms. Sanders.
13 So before I get into the --
14 JUDGE GIANNETTI: Just let me ask you, Mr. Lowenstein, how
15 much time are you reserving for surrebuttal?
16 MR. LOWENSTEIN: I will reserve 30 minutes with the
17 understanding of it may very well end up being less than that.
18 JUDGE GIANNETTI: Okay. Fine. So you may proceed.
19 MR. LOWENSTEIN: Okay. Thank you, Your Honor. Before I
20 get into the slides, I think what was striking about the reply brief and the
21 reply declaration was the extent to which it introduces new arguments and a
22 voluminous amount of new evidence.
23 Now, let's go to our Slide number 2. Can you see our slides, by the
24 way?
25 JUDGE GIANNETTI: Are you doing them -- yes, just make sure

1 you call out the slide numbers so that we can follow along. But I see that
2 you're also putting them up on the screen, so.
3 MR. LOWENSTEIN: Okay.
4 JUDGE GIANNETTI: But give us the slide numbers for the
5 record anyhow.
6 MR. LOWENSTEIN: Okay. Very good. So let's go to Slide
7 number 2. As Judge Giannetti himself, I believe, reminded us at the outset
8 of this hearing, the rules in PTAB proceedings are strict. Intelligent Bio-
9 System, the Federal Circuit tells us, Petitioners have an obligation to make
10 their case in a petition to institute. As a corollary, the Consolidated Trial
11 Practice Guide tells us, the Petitioner may not submit evidence or argument
12 in reply that could have been presented earlier, for example, to make out a
13 prima facie case of unpatentability.
14 Slide number 3. Here, however, in each of the three cases before
15 Your Honors, Petitioner has submitted over 40 new reply exhibits. I would
16 submit to Your Honors that that is an implicit admission the Petitioner did
17 not make its case in the petition to institute.
18 Slide number 3. Let's look at the reply declaration, 25,000 to
19 29,000 words. That is approximately twice the length of the petition. That
20 is not we proved our case in the petition, that's a we've got a lot of holes that
21 we've got to try to fill.
22 JUDGE GIANNETTI: Counsel, let me just stop you here. Is there
23 a -- isn't it true that a Petitioner has the right and the opportunity to present
24 evidence to rebut your Patent Owner response?
25 MR. LOWENSTEIN: They may respond to the arguments that we

1 make.
2 JUDGE GIANNETTI: So are you contending that this
3 voluminous, as you put it, submission is not responsive?
4 MR. LOWENSTEIN: Well, the question is -- I think you have to
5 go back to the trial practice guide.
6 JUDGE GIANNETTI: No. I read the trial practice guide. I'm
7 familiar with it. It does talk about rebuttal cases, though, and the ability to
8 rebut. And so my question to you is: are you just objecting to it on the basis
9 of volume or are you objecting to it as not being responsive?
10 MR. LOWENSTEIN: I would say that the volume is indicia on its
11 own. But you've got to take it case by case, of course.
12 JUDGE GIANNETTI: Well, there's no --
13 MR. LOWENSTEIN: Yeah.
14 JUDGE GIANNETTI: -- page limit on reply declarations is there?
15 MR. LOWENSTEIN: No, there's not. But on the other hand, if --
16 JUDGE GIANNETTI: What are you asking us to do? Are you
17 alleging that it's not responsive? That's my question to you.
18 MR. LOWENSTEIN: Well, but even if responsive, the question
19 then becomes, is it something you needed to put in the petition anyways to
20 make out, for example, a prima facie case? Not --
21 JUDGE GIANNETTI: Well, isn't that part of my question to you?
22 My question to you is: is it fairly responsive to arguments that you made in
23 the Patent Owner response?
24 MR. LOWENSTEIN: In substantial part -- and we're going to talk
25 about some instances further on this discussion.

1 JUDGE GIANNETTI: Okay.
2 MR. LOWENSTEIN: I believe it is evidence and arguments that
3 they needed to present earlier.
4 JUDGE GIANNETTI: Well, my question is: are they fairly
5 responsive? And that's what I would like you to focus on, whether they're
6 fairly responsive to arguments that you made. Now, I agree with you that
7 they did submit new evidence and that their reply declaration was on the
8 long side. But there's nothing in the practice guide that puts the page limits
9 on responses like that.
10 And so I think what I need to hear from you is rather than your
11 argument that it's too long, I want to know why it's not responsive.
12 MR. LOWENSTEIN: Yes. And perhaps we can talk about some
13 instances that -- if that's acceptable to Your Honor.
14 JUDGE GIANNETTI: And you didn't -- and let me just clear
15 another thing here. You didn't make a motion to strike or to exclude any of
16 that material, did you?
17 MR. LOWENSTEIN: In my experience before the Board, such
18 motions are generally not welcome. And to my understanding, motions --
19 JUDGE GIANNETTI: But they are permitted, whether they're
20 welcomed or not. The fact is that you didn't make one, did you?
21 MR. LOWENSTEIN: What I have heard from previous panels --
22 and I apologize if I --
23 JUDGE GIANNETTI: Yes.
24 MR. LOWENSTEIN: -- this applied that lesson from other
25 cases -- is motions to exclude should be based on evidentiary grounds.

1 JUDGE GIANNETTI: Well, what about motions to strike?
2 MR. LOWENSTEIN: In the cases that we have handled, we have
3 addressed it through objections to demonstratives, through briefing, through
4 argumentation.
5 JUDGE GIANNETTI: So the answer is that you did not make a
6 motion to exclude and you did not make a motion to strike.
7 MR. LOWENSTEIN: That is correct.
8 JUDGE GIANNETTI: Okay. You can proceed.
9 MR. LOWENSTEIN: We did, of course, object to the slides. And
10 we did, of course, present arguments about untimeliness in our certify, Your
11 Honor. So again, relatively --
12 JUDGE BELISLE: Counsel, before you go, just as a -- this is an
13 easy matter. These proceedings are recorded. And your video went from
14 being clear to fuzzy. So you're the only one being recorded right now that's
15 fuzzy. So if there's a way to get yourself in focus, it might make a -- there
16 you go.
17 MR. LOWENSTEIN: I'm sure my colleagues were trying to hide
18 some blemishes or something.
19 JUDGE BELISLE: You look better now.
20 MR. LOWENSTEIN: Thank you. We're in Los Angeles, of
21 course.
22 So as a related matter, there's another well-known rule -- I don't
23 need to belabor too long because I know Your Honors are often very
24 familiar with it -- is you may not incorporate arguments by reference in a
25 brief. If you want to make an argument, you've got to make the argument.

1 What you can't do is just have a conclusory sentence and then a long string
2 citation to, you know, loads and loads of paragraphs or lots of different
3 exhibits where you don't really explain what it is that you're talking about.
4 But that's what we see in the replies again and again. We have a
5 conclusory statement with a citation to, for example, 22 paragraphs of the
6 reply brief. We see this again and again and again. Similarly, we have a
7 conclusory statement with seven new exhibits cited. That's just an example.
8 And if you go through those --
9 JUDGE GIANNETTI: Counsel, I'm still wondering, what are you
10 asking us to do here? Are you asking us --
11 MR. LOWENSTEIN: All I'm asking Your Honors to do is to do,
12 frankly, what you yourself suggested at the start of --
13 JUDGE GIANNETTI: But there's no -- there's nothing before us --
14 there's no motion before us to strike.
15 MR. LOWENSTEIN: All I'm asking is that the Board apply it's
16 well-known, well set of rules against -- I'm trying --
17 JUDGE GIANNETTI: Which would be what? What would be the
18 endgame there if we were to apply the rules that you're pointing to, that this
19 evidence we will -- that we would ignore this evidence, is that what you're
20 asking us to do?
21 MR. LOWENSTEIN: To the extent it violates the rule against
22 improper incorporation by reference is got to be considered, yes.
23 JUDGE GIANNETTI: Well, but there's no motion before us.
24 MR. LOWENSTEIN: Right. But that -- as I believe, we all
25 understand those are the rules and motions to exclude -- to my

1 understanding -- again, are mostly on evidentiary grounds, not on --
2 JUDGE GIANNETTI: Motions to strike are not, though. Well, go
3 ahead with your argument. But I would prefer to hear you discuss the merits
4 rather than the number of pages in the record here.
5 MR. LOWENSTEIN: Well, yeah, you read my mind, Your
6 Honor. We're just about to turn to that.
7 JUDGE GIANNETTI: Good.
8 MR. LOWENSTEIN: I will handle the Foster grounds, with
9 Foster and Hayhurst, and Foster alone. Mr. Iancu will handle Orsini. And
10 then Ms. Sanders, our LEAP practitioner, will discuss Tajima.
11 So as we know, in the 212 and 215 case -- we're on Slide 9 -- we
12 are dealing with the Foster-Hayhurst Ground. Slide 10. And as I think I
13 heard my friend agree in his presentation, the arguments in the 212 and 215
14 cases are substantively identical. There's not a lot of difference in the
15 argumentation or presentation in the two cases.
16 There are three issues. The first --
17 JUDGE GIANNETTI: And also, you got to give us the slide
18 numbers.
19 MR. LOWENSTEIN: Thank you, Your Honor. We're on Slide
20 11. The first question that I'm going to address is the failure to prove that
21 Hayhurst is analogous art. Slide 12, I think as we know, when you're talking
22 about an obviousness combination, it only -- the reference only qualifies if
23 it's analogous. And as I believe it's undisputed, Petitioner has the burden to
24 prove it is analogous.
25 JUDGE GIANNETTI: I don't think that's undisputed.

1 MR. LOWENSTEIN: There is --
2 JUDGE GIANNETTI: What do you rely on for that, Counsel?
3 MR. LOWENSTEIN. All right. Let's go back to Slide 12. If we
4 see from Sanofi-Aventis from the Federal Circuit 2023 case, we agree with
5 Sanofi that the Petitioner did not carry its burden to argue that Gennes is
6 analogous and that also -- if we go back to the scope and content of the prior
7 art, Petitioner has the burden to prove the scope and content of the prior art,
8 including whether it's a fair game in an obvious (INDISCERNIBLE).
9 JUDGE GIANNETTI: Well, doesn't Sanofi actually support the
10 other side? I thought there was some statement in there. Let me see if I can
11 get a copy of the case up here. And I don't see that case now. Why don't
12 you go on with your argument? But I'm not sure I agree with you that the
13 burden falls on your opponent.
14 MR. LOWENSTEIN: I think -- I'm not --
15 JUDGE GIANNETTI: I think, maybe that's your argument. And
16 unless it was an anticipated -- unless it was an anticipated argument, I think
17 they have the right to contest that in their responsive papers.
18 MR. LOWENSTEIN: I don't disagree with that. I'm not disputing
19 that.
20 JUDGE GIANNETTI: All right. We're on the same page.
21 MR. LOWENSTEIN: Yes. I think what Your Honor is saying
22 is -- and I think there was some misapprehension on my friend's part. We
23 were taking the position that they had to prove it in the petition and that was
24 the end of the inquiry. When it comes to analogous art, that is not our
25 position. And if we go to that slide -

1 JUDGE GIANNETTI: So you're not contending that they forfeited
2 the argument of arguing that it's not a prior art; is that right?
3 MR. LOWENSTEIN: I am not.
4 JUDGE GIANNETTI: It's art.
5 MR. LOWENSTEIN: I am not.
6 JUDGE GIANNETTI: Okay.
7 MR. LOWENSTEIN: All I'm pointing out in Slide 13 is they did
8 not argue in the petition as a fact.
9 JUDGE GIANNETTI: All right.
10 MR. LOWENSTEIN: Okay. And we know -- Slide 14 -- that
11 there are two tests. There's the field of endeavor test, which I'm going to
12 discuss first. Slide 15, we know from the Federal Circuit's actual application
13 of that test it can be somewhat strictly implied. And we know that
14 references even in the same technological area, broadly speaking, may not
15 be found to be in the same field.
16 So In re Clay, which is the leading case, cited it in essentially
17 almost every analogous art decision from the Federal Circuit to this day.
18 That involved the case where you have one reference on storing oil, a gel
19 used in storing oil, and another reference on a gel used in extracting oil.
20 And the Federal Circuit said -- it's still a good law -- that it was clearly
21 erroneous for the Board to find that one was not -- was in the same field as
22 the other.
23 Relatedly, Slide 16, when --
24 JUDGE GIANNETTI: Counsel, we're pretty familiar with the law
25 here.

1 MR. LOWENSTEIN: Yeah.
2 JUDGE GIANNETTI: We don't need to be schooled on the law.
3 But would you address the question of what you think the field of endeavor
4 is here, the appropriate field of endeavor?
5 MR. LOWENSTEIN: Yes. I would just like -- and I'm cognizant
6 of what you just told me, but I hope you'll just bear with me on just --
7 JUDGE GIANNETTI: Okay.
8 MR. LOWENSTEIN: -- one more very brief discussion of law,
9 which we'll immediately transition to that.
10 JUDGE GIANNETTI: All right. Just keep it brief because --
11 MR. LOWENSTEIN: I will, I promise. If you could just give me
12 a second. Slide 19, there have been traditional sources that the Federal
13 Circuit has led to discern the field of endeavor. And these are what you
14 would expect. The written description, the claims, the title, the
15 specification, the field of the invention, the abstract, the structure and
16 function of the claimed invention, the background of the invention, that's
17 where we would all expect to discern the field of endeavor.
18 So let's look at those sources, as applied here, to discern the field
19 of endeavor to the '854 and for Hayhurst. Let's look at all of those fields: the
20 title, the abstract, the field of the invention, the background of the invention,
21 the summary of the invention, the claims in the '854. Slide 20, the field is
22 securing data. That's what the person of ordinary skill would discern
23 looking at the traditional sources the Federal Circuit has led to.
24 Slide 21. Let's look at Hayhurst, what is the title? Decentralized
25 Media Delivery. What is the abstract saying? A decentralized approach to

1 delivering a media file; the technical field, the field of electronic media
2 delivery, such as video-on-demand. Maybe focus on the remainder of that
3 clause. We'll get to that.
4 JUDGE GIANNETTI: Yes. Counsel, just -- let me just -- are you
5 contending that the media that's referred to here, the media file, that that's
6 not data?
7 MR. LOWENSTEIN: I'm not suggesting that at all, Your Honor.
8 JUDGE GIANNETTI: So why doesn't it fall within the definition
9 of securing media -- of securing data? Why wouldn't securing a media file
10 be an example of securing data?
11 MR. LOWENSTEIN: Well, I think when you look at each of the
12 sources we've been told to look at, they all sing from the same hymnal and
13 they all refer to decentralized media delivery. And so I believe --
14 JUDGE GIANNETTI: Listen, you didn't answer -- you're not
15 answering my question. My question is: why wouldn't a person of ordinary
16 skill in the art consider a media file data?
17 MR. LOWENSTEIN: I am not disputing that, Your Honor. I
18 believe a person of ordinary skill in the art would consider a media file to be
19 data.
20 JUDGE GIANNETTI: You can continue.
21 MR. LOWENSTEIN: Okay. So if you --
22 JUDGE REPKO: I have a question, Counsel, if you don't mind.
23 On this issue of decentralized media delivery in particular, I guess I asked
24 the similar question to Petitioner about page 3 of their reply in the 215 case.
25 They cite the specification of the challenged patent.

1 And one of the things they noted is they say the disclosures apply
2 to peer-to-peer file sharing and video broadcasting. So I mean, that seems to
3 suggest that the field of the challenged patent is also decentralized media
4 delivery in a way, right?
5 MR. LOWENSTEIN: I don't believe there's any dispute from my
6 friend -- both parties, both experts, to the extent they addressed it at all. We
7 all agree that the field for the '854 is securing data. So I don't think that's a
8 position that either party has presented or defended.
9 JUDGE REPKO: What about on page 3 of their reply in the 215
10 case, the footnote 3?
11 MR. LOWENSTEIN: Yeah. I'm looking at that. But I don't see
12 them as saying that is the field of endeavor for the '854. And what I take
13 their argument to be is they told their expert to just adopt the '854 field. And
14 that's what he says in his declaration and that's what they argue.
15 But let's say peer-to-peer file sharing, I don't think that's Hayhurst's
16 field. And I don't think anyone argues that's Hayhurst's field either because
17 it's not peer-to-peer. It's not file sharing, as I understand that term. And
18 certainly not peer-to-peer, as I understand that term. It's not video
19 broadcasting either in -- at least in the sense of a real-time broadcast.
20 And so even if that were the '854's field, which I don't think they've
21 fairly argued -- I understand the footnote that you're identifying -- I don't
22 believe that would be Hayhurst's field either.
23 JUDGE REPKO: I mean, they talk about the -- essentially, the
24 geographic separation of these storage facilities, just storing things in a
25 decentralized way in the challenged patent; isn't that correct? I mean, isn't

1 that the idea behind the whole encryption scheme? Is it the sort of
2 decentralized storage (CROSSTALK) in that way?
3 MR. LOWENSTEIN: In the '854 or Hayhurst?
4 JUDGE REPKO: In the '854, they talk about geographical
5 separation. And then the data, it could be anything I guess. But they make a
6 point to say that it's video data in that column, column 81.
7 MR. LOWENSTEIN: So it's certainly -- the '854 discusses
8 distributing data shares in different locations. That's an aspect of the
9 disclosure. But I think when the question is what is the field, we're not
10 looking so much to the particular solution or the particular application. It's
11 going to be a little bit broader than that. It's going to be something like
12 securing data.
13 And I think if it was something like peer-to-peer file sharing or
14 video broadcasting or at least sticking files in different locations, that would
15 be a little bit too granular. It wouldn't fairly capture the field of the '854, in
16 my humble opinion.
17 JUDGE REPKO: And then the technical field here that you're
18 citing here on page -- I guess, it's paragraph 12, they do mention secure
19 handling and storage. So I mean, I guess it depends what you're broadening
20 out there, right? It seems like Hayhurst could also be kind of characterized
21 in that way. You're focusing on the media aspect, I guess, of it.
22 MR. LOWENSTEIN: Yeah. Because that's what I think we see
23 from the title, the abstract, the, you know, technical field, the figures, the
24 background, the invention, the summary of the invention of the claims. So a
25 person of ordinary skill in the art picks up Hayhurst, what are they going to

1 think of the fields? And I think they're going to think it's decentralized
2 media delivery.
3 JUDGE GIANNETTI: Wait a second, Counsel. I'm looking at the
4 petition and I thought that, in our institution decision, I thought that the
5 agreed upon person of ordinary skill was a -- let me just see here, give me a
6 second here. Give me a minute to find it.
7 Here, a person of ordinary skill, Petitioner asserted that a person of
8 ordinary skill in the art would have had at least a bachelor's degree in
9 computer science, computer engineering, or related field with three years of
10 experience in the area of securing data from unauthorized access or use.
11 And that was -- I don't believe that the Patent Owner refuted that. I think
12 you adopted that.
13 So why doesn't that broad statement of what the person of ordinary
14 skill would know, why wouldn't that encompass these references that you
15 contend are not analogous art?
16 MR. LOWENSTEIN: So that's a statement of the level of skill of
17 the person of ordinary skill in the art, which --
18 JUDGE GIANNETTI: Right. But isn't that what analogous art is
19 all about, is what a person of ordinary skill in the art would have looked to
20 and what field they would have looked to for help in solving a particular
21 problem?
22 MR. LOWENSTEIN: But I didn't -- I don't see a lot of daylight
23 between what you described as the field for purposes of a person for
24 ordinary skill in the art and what we say, and I believe the Petitioner doesn't
25 dispute, is the field for the '854, which we would say is securing data.

1 JUDGE GIANNETTI: When I start hearing about, you know,
2 specifics of media delivery and that sort of thing, it seems to me that all falls
3 within the scope of -- and I think we discussed this -- falls within the scope
4 of securing data. So why isn't this something that that this hypothetical
5 person would feel that they would look to?
6 MR. LOWENSTEIN: I think in the interest of time, I do feel
7 compelled to make sure there's enough time for my colleagues to argue and
8 I -- so I can address all the issues. But I think the essential position that
9 we're presenting is that when a person of ordinary skill, when they look at
10 the traditional sources the Federal Circuit has looked to, discerned the field
11 of endeavor for the '854, which I don't respectfully believe is disputed, and
12 Hayhurst, that person is going to conclude, weighing those traditional
13 sources, that these are not within the same field. That's our position --
14 JUDGE GIANNETTI: As the patent?
15 MR. LOWENSTEIN: Correct. I think that's -- this Slide 22,
16 essentially, sums up our position when coupled to the body of Federal
17 Circuit case law on how to discern the field of endeavor.
18 JUDGE GIANNETTI: All right. I guess we have your position on
19 that. Any other questions for the panel before you move on to some other
20 subject?
21 MR. LOWENSTEIN: Okay. Thank you, Your Honor.
22 JUDGE GIANNETTI: Okay. Thank you. Let's hear you on the
23 merits.
24 MR. LOWENSTEIN: Okay. So just one last point on reasonable
25 pertinence and then I'm going to move on, if that's okay.

1 JUDGE GIANNETTI: Please.
2 MR LOWENSTEIN: I heard, Slide 30 -- and I may have misheard
3 my friend. So I apologize if I misunderstood him. But I thought I heard him
4 say that it doesn't matter for purposes of reasonable pertinence what problem
5 Hayhurst is trying to solve. But that's not correct.
6 If we look at what the Federal Circuit held in Donner just five
7 years ago when addressing whether he references analogous under a
8 reasonable-pertinence theory, the problems to which both relate must be
9 identified and compared. And we don't believe Petitioner argue with the
10 burden did that. So I will, with that -- if it's acceptable -- move on to the
11 combination art.
12 JUDGE GIANNETTI: Please do.
13 MR. LOWENSTEIN: Okay. So I think we saw from my friend's
14 discussion that we're focused on the limitation storing on different storage
15 devices. It comes up in both the '116 and the '854 on Slide 37. Slide 38, it's
16 not disputed that Foster does not store data chunks on a plurality of different
17 storage devices.
18 Slide 39. The combination is Foster's technique of encrypting
19 portions of a data set with Hayhurst's technique of storing the encrypted data
20 on different storage devices. Now, heard a lot of talk about video-on-
21 demand in my friend's discussion. But that was not the focus of their
22 combination. Again, what they're combining is Foster's encrypted content
23 units with Hayhurst's distributed storage techniques.
24 But I think what we're going to find is -- the really fundamental
25 question is: would a person of ordinary skill in the art, with Foster in hand,

1 with Hayhurst in hand, be motivated to combine -- to make this
2 combination? Or is it going to be so damaging to what Foster is trying to
3 achieve, the benefits that it entails, the benefits versus the drawbacks the
4 person of ordinary skill isn't going to want to do it?
5 Part of that analysis is a POSITA generally is not motivated to
6 make a reference inoperable for its intended purpose. And a POSITA is not
7 going to be motivated to undesirably change the references of principle of
8 operation.
9 Now, I heard a lot about Foster not being limited to this, not being
10 limited to that. Foster is not limited to real-time streaming. Foster is not
11 limited to live cable television. I would respectfully present that that's a
12 little bit of a red herring. We never argued that Foster was limited to real-
13 time streaming. We never argued that Foster was limited to cable television.
14 That is not our position. We have never presented that position.
15 That seemed to be the bulk of the discussion. To my friend, that seemed to
16 answer all questions. I would submit that it does not.
17 Let's look at what Foster is actually about. So Foster has a --
18 JUDGE GIANNETTI: Counsel, you need to give us the slide
19 numbers you're using.
20 MR. LOWENSTEIN: I'm sorry, Your Honor. There are two
21 things I've always failed to do in my career, one of them is mentioning slide
22 numbers. So I apologize.
23 JUDGE BELISLE: Counsel? And also while we have this just
24 slight break, because our transcripts are publicly available, ultimately, in the
25 record and stuff, I think it would be better to use terms like Petitioner's

1 Counsel or Opposing Counsel, not my friend. Because somebody reading
2 that is not going to know who you're referring to, somebody at your table or
3 who. So perhaps just use Opposing Counsel or Petitioner's Counsel.
4 MR. LOWENSTEIN: Very good. I hope Mr. Nieberg will bear
5 no offense. So if we look at Foster, we look at the title, the abstract, the
6 background, the invention, the summary of the invention, what is it about?
7 It's about attaching a title content to the encrypted content that it decrypts.
8 That's in the title, that's in the abstract, the field of the invention, attaching a
9 title key to encrypted content for synchronized transmission.
10 Both experts agree. Let's look at the deposition testimony of Dr.
11 Bhattacharjee. Why the synchronous transmission to receive Foster's
12 random access to content? That is sort of the whole invention of Foster.
13 Again, encrypted content, you synchronously transmit it with the key that
14 decrypts it. Okay. That's what it's about.
15 Next, Slide 43. Why does it do that? Foster synchronously
16 transit -- transmits the key with the data it encrypts because the prior art
17 systems that didn't do that suffered from undesirable delays, particularly
18 when it comes to randomly accessing content. And the example the patent
19 gives randomly -- or the application I should say, gives of randomly
20 accessing content is you try to change the channel and does the image
21 appear.
22 I'm not saying it's limited to that. But that's what it's talking about.
23 It doesn't like the delays. It doesn't like the latencies. And it's because
24 you've got the encrypted content and you're fumbling around looking for the
25 key. Where is the key? So we're going to send the encrypted content with

1 the key right away.
2 To Slide 44, address the undesirable delays, that is what Foster is
3 all about. If you read Foster, if a person of ordinary skill in the art reads
4 Foster, that's what Foster is trying to achieve. Submit the key with the data
5 it decrypts to avoid searching around for the key and to avoid delays so you
6 can randomly access content fast. That's Foster.
7 As an application of that and an illustration of how well Foster
8 does what it wants, Slide 45. Foster says that you can do this in real-time
9 streaming. You change the channel, it appears, no delay. That's what Foster
10 is about. 46, in the figure, that is the heart of their combination that they
11 turn to again and again, Figure 8, that's about encryption of an elementary
12 stream. And so even their use of Foster is in this streaming context.
13 But here's the problem with their combination. You have a
14 reference, Slide 47, Foster on the one hand that says, look, we've got to send
15 the key with the data it decrypts so we can access content faster. But the
16 combination is going to destroy that entire feature of Foster because
17 Hayhurst is not concerned with synchronous transmission. It's not
18 concerned with avoiding delays. It's not concerned with allowing you to
19 change the channel immediately to get right to it.
20 Slide 47. Hayhurst is about addressing the bandwidth concerns
21 from the content owner. Foster is not the content owner. Foster is a
22 middleman that applies encryption before setting it off. But the problem
23 with this and the problem that affects their combination is Hayhurst is such a
24 slow, meandering, laborious process that it will prevent Foster from doing
25 the very thing that it desperately wants to do. It will prevent Foster from

1 randomly accessing content quickly.
2 So Slide 48, I think we know this by now. But just to set it, they're
3 worried -- Hayhurst is worried about bandwidth demands, the cable system,
4 for example -- and so it's trying to address that problem of limited bandwidth
5 in the video-on-demand context. But as we just discussed, Hayhurst is not
6 about real-time streaming. That is nothing at all -- it has nothing to do with
7 real-time streaming. Hayhurst is specifically about the video-on-demand
8 context.
9 So let's look at how Hayhurst works. You want to see a movie,
10 let's say Goldfinger. So you've got a media file, that's complete. I think Mr.
11 Nieberg agrees with me on this, that's what sort of Hayhurst is directed
12 towards -- you're not watching the Super Bowl because that's in real time.
13 To use Hayhurst's method on the Super Bowl, you'd have to wait until the
14 Super Bowl ended, then distribute Hayhurst to a thousand different
15 households and then somehow reassemble it. It's not going to work in that
16 context. I don't think that's actually disputed.
17 So let's look at Hayhurst's intended operating. You take a movie
18 like Goldfinger, and rather than just stream it to a recipient, as Foster would
19 immediately, I want to see it fast. I click -- let's say we're in the video-on-
20 demand context. In Foster, you get it right away. Immediately, you're
21 listening to the guitar. That's how it would work in Foster.
22 That's not how it goes in Hayhurst. And that's not how it's going to
23 go in their combination. Because what Hayhurst says is rather than be able
24 to watch Goldfinger right away, what we're going to do is we're going to
25 slice it up into a thousand different or more segments, 10,000. And we're

1 going to spread that into individual people's homes, into their set-top boxes.
2 And that way, we've beneficially helped the bandwidth for the MGM or
3 whoever runs Goldfinger now.
4 So when one of those set-top boxes launch Goldfinger, it says to
5 the server to pay her server. Can I please get the segments for Hayhurst --
6 I'm sorry, for Goldfinger? The server contacts the thousand -- 10,000
7 different homes, different set-top boxes. Can you please send the requesting
8 set-top box your segment or segments of Goldfinger?
9 But that's not the end of it. That would be bad enough, but that's
10 not the end of it. There are going to be missing segments, lots of missing
11 segments. Why? Because someone's power went out in their home, they're
12 no longer a subscriber, the Internet connection is down, they've opted out,
13 whatever it is. So the requesting set-top box then has to go back to the
14 server and say, hey, I'm missing these 700 segments. So Hayhurst server
15 says, okay, let's go to the backup servers and see if they've got it -- or backup
16 set-top boxes to see if they have it.
17 Now, Petitioner's Counsel tries to spin this as a virtue. We have
18 redundancy, isn't that great? But that is -- that's like the old lady who
19 swallowed the spider to catch the fly, their combination creates this problem
20 for Foster. Foster does not need redundancy. Foster's just streaming from
21 Foster's system to the recipient or the content attaches the encryption to the
22 recipient, drop the packet, and you just resend it.
23 It's a consequence of this distributed method where, oh, hey, Joe
24 Smith has his power out, that's why you need the redundancy. So adding
25 Hayhurst to Foster is not solving some problem. In Foster, at most, it's

1 addressing a problem that its own combination introduced. And it --
2 JUDGE REPKO: And so I think Petitioner kind of anticipated this
3 argument in a way in the petition when they said that -- I mentioned this in
4 the questioning of Petitioner's Counsel -- they said in pages 64 and 65 that
5 the Foster's content units are individually accessible and agnostic to where
6 and how they are stored compared to other content units and, thus, were
7 compatible with being stored on multiple separate storage devices.
8 What's your response to that statement from the petition? They
9 don't -- it doesn't matter where they're stored but it still works the same way.
10 MR. LOWENSTEIN: Well, I'm not -- I don't mean to miss the
11 point, but the storage from what context? So first, Foster on its own, to my
12 understanding, gets the movie file or whatever it is from content owner. So
13 it's being stored on the content owner, it applies its encryption and sends it
14 directly. And it could be sending it to any number of different homes for
15 immediate streaming or whatever it would be. And Foster does say that it
16 could be sent for transmission or storage. It doesn't care.
17 So in a direct one-to-one Foster system to a recipient, Foster
18 doesn't care whether it's just sending it or it's sending in the recipient that
19 stores it. But it can be stored in multiple households when you look at --
20 when you take a step back, we look at that from the system as a whole.
21 Does that answer your question or --
22 JUDGE REPKO: They work differently. I realize that Foster
23 works a little differently than Hayhurst. That's kind of the point, right? I
24 mean, it depends on what type of attack you're trying to prevent. Here
25 they're saying we want to just take Foster's content units and distribute them

1 as described in Hayhurst. And that's not necessarily going to break
2 anything. Because really, Foster's content units, it doesn't matter where
3 they're stored. They're agnostic the where and how they're stored. That's
4 what they said on pages 64 and 65 of the petition.
5 MR. LOWENSTEIN: But I think the thing that Foster is not
6 agnostic about is it doesn't allow you to get the key and the data right away
7 so you can randomly access content. That's the whole point. So if you're
8 doing anything that's going to disrupt that, a person of ordinary skill -- I'm
9 hard-pressed to see why a person of ordinary skill in the art is going to want
10 to do that.
11 MR. REPKO: Yeah. I want to hear more about that, the keys and
12 how the key is managed. I think that you're -- that Petitioner's Counsel kind
13 of spoke to that and gave their opinion about that. And I think this -- the
14 idea that you can distribute the content on different devices, I think -- I don't
15 see why Foster's content couldn't be broken up in that way.
16 It's I guess the key management that I do have some questions
17 about. I'd like to hear more about that. I don't want to --
18 MR. LOWENSTEIN: I think you know our position on
19 everything. But just very briefly, to recap, so a person of ordinary skill in
20 the art reading faster wants to go as fast as possible so you can randomly
21 access content. If you spread it to the winds of this cumbersome, very slow
22 process, you're destroying that core benefit of Foster. So that's my response
23 to that. Let me, if I may, turn to the security point that I think you'd like to
24 hear about.
25 Okay. So there's a further problem with the Foster-Hayhurst

1 combination, which is going to undermine Foster's security. We're on Slide
2 56, turning to Slide 57. Now, let's look at Foster alone before Hayhurst.
3 Foster alone has pretty good security. As we heard from Mr. Nieberg,
4 Foster not only has an encrypted key but also a key encryption key. But it's
5 not just that, Foster teaches that you can re-encrypt the encryption key
6 whenever you want.
7 Now, here's an important point. When it's in Foster's system, not
8 once the horse has left the barn, not once it's been distributed to a thousand
9 different households, but when it's in Foster's system, before you send it out,
10 you can change the key encryption key. That's the benefit. Because if you
11 think one has been compromised, you can change the key, KEK.
12 Slide 58. There's another benefit to Foster's system before you've
13 polluted it with Hayhurst. Foster's system allows you to have KEKs that are
14 specific to each individual subscriber. Because as I think I heard Mr.
15 Nieberg argue -- or agree at least -- there's a key management block that's
16 sent to the users in advance. And so you can craft key encryption keys that
17 are specific to each recipient. And here's the problem, you can't do either
18 one of those things in the combination.
19 We're on Slide 59. So under the Foster-Hayhurst combination,
20 you're doing all of your encryption before it leaves Foster's system and it's
21 distributed to these storage device by the system of Hayhurst -- or these set-
22 top boxes, I should say. And because you're applying your title keys, your
23 key encryption keys -- key or keys -- at that point, before they've left Foster's
24 system, you don't have that flexibility. You can't change the key encryption
25 key because it's already left the system. The horse has left the barn.

1 Foster is not saying once you've sent it out you can then change the
2 key encryption key. But Foster is saying you can change the key encryption
3 key without re-encrypting the content while it's in its system. And you can't
4 have specific KEKs to each user because any of the users can request that
5 movie. So any user that can request the movie is going to have the same
6 KEK or KEKs to do that. And by KEK, I mean K-E-K, capital K, capital E,
7 capital K.
8 JUDGE REPKO: Yeah. I think this is an interesting point. And I
9 asked about this earlier too. And I guess one of the things they would say,
10 well, you know, if I understood them correctly, essentially, there's a trade-
11 off. You know, you still -- authorized users are still going to get that key.
12 So the concern that you have, if I understand you correctly, is that
13 authorized users will -- the data will be shared across authorized users; is
14 that correct? Is that the concern here with the -- introducing a security issue
15 in Foster?
16 MR. LOWENSTEIN: Limited within the realm of security, there
17 are two concerns. The first concern is that unlike Foster's system alone,
18 once you've combined it with Hayhurst, you can't re-encrypt the title keys,
19 you know, in real time because it's already been sent out. So if you think
20 something's been re-encrypted -- I don't know, maybe you have to somehow
21 pull back all of the segments used and somehow re-encrypt everything and
22 send it out.
23 It's not clear on how you could do that. But you can't just like you
24 can in Foster, just re-encrypt it with the next packet. I think there's a
25 problem, let's change that to the next packet. You can't do that. And then

1 the other problem is you can't have it unique to each user. It's, at most,
2 going to be unique to the movie. Because any of those views you've already
3 encrypted, your title keys, your key encryption key, you've spread it to the
4 wind.
5 And any of those tens of thousands of subscribers can request
6 Goldfinger at any point in time. And because you've already done that,
7 you've already done your encryption work, which is kind of set in stone at
8 that point, you can't have two generous unique key encryption keys for each
9 subscriber. Does that make sense?
10 JUDGE REPKO: Yeah. That's what I'm interested in. Thank you
11 for clarifying that -- your position on that.
12 MR. LOWENSTEIN: Very briefly, I'll say, in some of the papers
13 they say, oh, you could do it without re-encrypting the content itself. But
14 that's precisely what Slide 63, Foster says you don't want to do because re-
15 encrypting the content itself will be significantly more time consuming or
16 consume more resources than just re-encrypting the title key.
17 Again, I think we know this by now. It's not just looking at trade-
18 offs. I heard discussion of trade-offs. What you have to do is you have to
19 weigh the benefits and the drawbacks and ask would a POSITA fairly be
20 motivated to do this at the time in view of the benefits and the drawbacks,
21 not that are trade-offs. That's not the end of the inquiry.
22 Do the benefits outweigh or how does that calculus work? And I
23 think what we see here, Slide 66, is there are a lot of drawbacks. There are a
24 lot of drawbacks to this combination. You're making it much, much slower.
25 You can't have live television. I'm not saying it's limited to that, but you

1 can't have it anymore. You can't have real-time streaming. You have less
2 security for the reasons I just discussed. You have delays.
3 And for what benefit? For more bandwidth? When does Foster
4 say that is a problem? For redundancy? That's the old lady who ate spider
5 to catch the fly. That's the problem resulting from the combination itself.
6 That --
7 JUDGE REPKO: I guess on the right-hand side here, the
8 redundancy does create some security, right? Because the -- each single
9 segment has less value than the entire movie for example, right? So there
10 is -- it's more than just better bandwidth, right? What do you say about that
11 aspect of the security?
12 MR. LOWENSTEIN: Yeah. I don't mean to nitpick. I will
13 address that. I don't think that falls in the bucket of redundancy. I think in
14 the bucket of redundancy, they specifically mean we have a missing
15 segment, so there's our backup packet here. But I think what you're really
16 talking about is if you take Hayhurst's system and you've split up the
17 segments across the 10,000 different subscribers, because each one has only
18 a minute amount maybe it's not that valuable. I think that's, essentially, what
19 you're pointing to.
20 JUDGE REPKO: Yeah. Because you have on the left-hand side
21 the less security. And I'm wondering if that less security is offset by the fact
22 that we are distributing pieces of it rather than distributing the entire thing
23 like you do in Foster --
24 MR. LOWENSTEIN: Yeah.
25 JUDGE REPKO: -- in streaming because that's --

1 MR. LOWENSTEIN: I agree that that's a pretty good method.
2 But it's no better than Hayhurst. If anything, it's marginally -- quite
3 marginally. But it marginally works. So if we take, let's say Goldfinger. In
4 Foster system, MGM has Goldfinger, a set-top box wants to see Goldfinger,
5 request it.
6 So Foster's going to say, okay, give me Goldfinger, pass the keys,
7 send them off. Those keys are not sitting out there. And that -- those
8 segments, they're not just sitting out there waiting to be attacked. They're
9 only sitting out there waiting to be attacked in Hayhurst's system.
10 So in Hayhurst's system, MGM has Goldfinger. And then the
11 cable system disperses it to the winds. And it's quite right that it's pretty
12 secure because who cares about, you know, one little packet. But Foster
13 doesn't have the one little packet out there because it's sending it in real-time
14 streaming.
15 JUDGE REPKO: Thank you.
16 JUDGE BELISLE: Counsel, perhaps, just to put some focus on
17 this, I would like to hear the response to the questioning of Petitioner's
18 Counsel regarding that execution of code for storing the chunk on what, I
19 believe from your briefing, you know, was originally to the storage device
20 which diagrammatically was outside the computer, and then that seemed to
21 shift in reply to storage inside the computer. Can I get your response to
22 that?
23 MR. LOWENSTEIN: I almost broke my neck, nodding in
24 vigorous agreement with your questions during my -- Mr. Nieberg's
25 questioning. And I think you're quite right. How could the processor on

1 Foster's system be executing code to tell the whatever storage device might
2 be on the recipient, you got to store that. And I share your confusion, it
3 doesn't make any sense to me. And I don't believe we ever saw any valid
4 explanation of that.
5 And in fact, if you look at the content unit and the encryption key
6 and the header, you look at what's in that, there's no instruction in there that
7 says, hey, can you store this here? I would analogize Foster's system is sort
8 of like if you order Uber Eats or from Costco, whatever, and they bring you
9 some food, they don't care whether you eat it, put it in the refrigerator, or
10 feed it your dog, whatever. It's completely indifferent. There's no executing
11 code to instruct the store -- or to perform to instruct, I should say -- is what I
12 meant to say.
13 And then I think you're right that that was not a part of their
14 anticipation argument. And they say it would be obvious to store it in
15 Foster's system. But I think you're quite right that when you look at the -- I
16 think it's Bus 402, Memory 402. And yeah, that's a memory. And it tells
17 you what's stored in there, but never does it say it's storing content or content
18 units.
19 And so then the question is, well, would you be motivated to do
20 that? And I'm not sure why you would. Because the way Foster's system
21 works is it gets the protected content or the content you want to protect from
22 a content owner; and then it does its encryption, sends it.
23 And what is the point of storing it there? We know that it's fast
24 enough to act in real time, as you change the channel, it's there. You could
25 do it and access it at any network packet. So why would you create an

1 additional security risk to -- by storing the content on that system when you
2 don't need it? And I would imagine MGM is quite sensitive about where
3 you're storing its content.
4 So does that fairly answer your questions, Your Honor?
5 JUDGE BELISLE: Yeah, I think so. I think you agree.
6 MR. LOWENSTEIN: Oh, yes.
7 JUDGE BELISLE: And I guess my follow-up to that is just do
8 you -- is it Patent Owner's position that the argument about storing the
9 chunks sort of within the computer, that that's a new argument, a bad
10 argument, or both a new and a bad argument?
11 MR. LOWENSTEIN: It's at least a bad argument. It is a new
12 argument to the extent it is arranged as a anticipation argument. And my
13 colleague is directing me to Slide 101. And I think this shows it quite well.
14 If you see what they said in the petition, each content unit is stored on a
15 receiver at Recipient 430. And then the reply, they point to the storage
16 device in the RAM. So it is a new argument from an anticipation standpoint.
17 It is a bad argument from an obviousness standpoint. That's it.
18 Okay. So can we just move -- can go back to where we were?
19 There was some discussion about DRMS. And so they -- I'm not quite sure
20 what the point of it is. We're not disputing that DRMS is discussed in
21 Foster's, but it's quite clear that it's discussed as background art, at least so
22 here's what they say in their reply in 73, 74.
23 DRMS is discussed in the background art of Foster. And it's
24 saying this is the deficient prior art, this is the prior art. It doesn't
25 synchronize the encrypted content with the key. And so you've got these

1 problems of latency and delay. And so it's no good. And it cannot practice
2 Foster's invention because we see there's a license server that's separate from
3 a streaming media server. So it's not configured to send at a single
4 transmission a synchronized transmission of the encrypted content with the
5 key used to encrypt it.
6 Next, Slide 75. Again, from Foster, "The DRMS fails to provide
7 synchronized delivery of the content with the keys used to encrypt the
8 content." And what again, from their own expert's lips, was the whole
9 invention of Foster? Synchronous transmission of the encrypted content in
10 the keys that's present in Foster's Figure 8, for example, not present in
11 DRMS. It is the prior art. I'm not sure what dispute there could be about
12 that.
13 Now, we also had discussion of the packets and payloads. There's
14 a typo here. This argument, I believe, also applies in the 212 case. So I
15 apologize for that. It says 214 and 215. It also applies in the 212. We're on
16 Slide 78.
17 And Slide 79, again, the question really is: is a network packet,
18 like an MPEG network packet, is that shown to be a data chunk or a share?
19 Their argument, Slide 80, is that the packets and payloads from, for
20 example, Foster's elementary stream is a chunk or a share.
21 Next slide, I will respectfully submit -- Slide 81 -- that the
22 argument, at least in the petition, was that it's (INDISCERNIBLE). It's a
23 share -- a packet is a share or chunk because we say so. Not a lot of proof
24 there. And it's not disputed that the types of packets that we're talking about,
25 these are just the default packets associated with the MPEG data protocol.

1 It became a little fuzzy again. If someone could --
2 JUDGE BELISLE: Counsel, this is Judge Belisle. Is Patent
3 Owner disputing that Foster has a stream of data, and that stream of data is
4 broken into something less than the entire stream for transmission?
5 MR. LOWENSTEIN: Absolutely not.
6 JUDGE BELISLE: Okay. So we're -- the argument is over
7 terminology, semantics. As to what it calls -- well, I mean, obviously, we're
8 in patent law. But I mean, the reference itself is disclosing a stream of data
9 that is broken up, and those broken pieces are encrypted. Do you agree with
10 that?
11 MR. LOWENSTEIN: Absolutely.
12 JUDGE BELISLE: Okay.
13 MR. LOWENSTEIN: It's a question of client construction and has
14 the Petitioner proven that these network packets are shares or chunks. We
15 can call it semantics, but then we don't (INDISCERNIBLE).
16 So if we look at Slide 83 --
17 JUDGE GIANNETTI: It's Judge Giannetti. Has either side
18 proposed a construction for this term, for chunk or whatever?
19 MR. LOWENSTEIN: I may have --
20 JUDGE GIANNETTI: I don't recall seeing it. So you say it's a
21 claim construction question, but it wasn't one that was raised by either side.
22 MR. LOWENSTEIN: Well, I sort of implicitly thought I heard
23 one from Petitioner's Counsel in the presentation this morning. I will agree
24 with Your Honor that we're arguing from the vantage points of you only
25 have to construe the claims to resolve the dispute in front of you. And what

1 we're saying is they haven't shown that a POSITA would consider a network
2 packet to be a data chunk. But when you look at it --
3 JUDGE GIANNETTI: But isn't the whole point of packet
4 technology that you divide something up into smaller pieces and send -- you
5 send those separately. Isn't that the whole point of it?
6 MR. LOWENSTEIN: There's no dispute that there is a movie. It's
7 been divided into packets.
8 JUDGE GIANNETTI: Yes.
9 MR. LOWENSTEIN: Yes. There's no dispute about that. The
10 only question is whether a POSITA would consider that to be a chunk or a
11 share. That's the only dispute. And what I would say is the patent doesn't
12 suggest that.
13 JUDGE GIANNETTI: And why wouldn't it be a chunk? I mean,
14 it sounds pretty chunky to me. That's the whole point of it.
15 MR. LOWENSTEIN: I'll be brief. But I think what we see --
16 JUDGE GIANNETTI: Yes. Just tell me in 25 words or less why
17 I'm wrong about that.
18 MR. LOWENSTEIN: Because when the patent refers to a packet,
19 it refers to the packet as the thing that's being divided into shares or chunks.
20 That's the usage in the patent.
21 JUDGE GIANNETTI: I see. Thank you.
22 MR. LOWENSTEIN: And we're on Slide 84. And when we look
23 at the usage of the literature we see, again and again --
24 JUDGE GIANNETTI: Well, at some point, though -- at some
25 point, the thing that's been packetized was an integrated piece of data, wasn't

1 it? That's the whole point of it. So --
2 MR. LOWENSTEIN: Yes.
3 JUDGE BELISLE: So Counsel, putting all your literature aside,
4 the claim itself uses the term data chunk, correct? Uses chunk.
5 MR. LOWENSTEIN: It does, yes.
6 JUDGE BELISLE: But the specification never uses the term
7 chunk, correct?
8 MR. LOWENSTEIN: I believe it uses the term share. Right.
9 JUDGE BELISLE: So right off the bat, the spec uses share and the
10 claim uses chunk.
11 MR. LOWENSTEIN: Yes. But I don't --
12 JUDGE BELISLE: The trouble is it's not disclosed anywhere in
13 the spec.
14 MR. LOWENSTEIN: Although there's a relationship between
15 shares and chunks and the claims, for instance, where it says you, you know,
16 create chunks, generate chunks by preserving the shares, encrypting the
17 shares. So there was a clear relationship, in my view, between chunks and
18 shares as reflected in the disclosure itself.
19 So I take your point. You're right that that's just the same word.
20 But I think we've all seen in patents where you're not using exactly the same
21 word, but yet we know that when the claim says it's referring to something
22 similar. And I don't think there's a whole lot of daylight between a share and
23 a chunk, particularly when some of the claims say you generate a chunk by
24 breaking it into shares and then you --
25 JUDGE GIANNETTI: Or a packet.

1 JUDGE BELISLE: Right. But I guess, Counsel, my point there
2 for just going down that little road was simply that the claim is data chunks.
3 The claim is not a packet.
4 MR. LOWENSTEIN: And shares.
5 JUDGE BELISLE: And shares.
6 MR. LOWENSTEIN: Yes. But --
7 JUDGE BELISLE: But not packet. The packet is not recited in
8 the claim.
9 MR. LOWENSTEIN: I don't believe it is.
10 JUDGE GIANNETTI: So, Counsel, are you going to address
11 Tajima at some point, or are one of your colleagues are going to be talking
12 about it?
13 MR. LOWENSTEIN: Give me just --
14 JUDGE GIANNETTI: The Foster-Tajima grounds -- Tajima.
15 MR. LOWENSTEIN. Okay. So --
16 JUDGE GIANNETTI: Are you going to be addressing that, or is
17 one of your colleagues?
18 MR. LOWENSTEIN: I think we -- I guess it's a question for
19 Judge Belisle because the next issue after this is sort of the thing we were
20 just talking about. So I guess, before I --
21 JUDGE GIANNETTI: So I'm not asking you to jump ahead. I
22 just want to make sure that you leave time to discuss that.
23 MR. LOWENSTEIN: Oh, no --
24 JUDGE GIANNETTI: At least one of your colleagues, if you're
25 not going to do it.

1 MR. LOWENSTEIN: Well, I think I would ask Judge Belisle,
2 have I answered all your questions on the questions about getting code for a
3 processor and storing and the obviousness? Because that was the last issue I
4 was going to discuss before turning it to Mr. Iancu. But I want to make sure
5 I haven't --
6 JUDGE GIANNETTI: By all means, answer Judge Belisle's
7 question.
8 JUDGE BELISLE: I get your position. Thank you.
9 MR. LOWENSTEIN: Okay. With that, I will pass the mic.
10 Thank you, Your Honors.
11 MR. IANCU: Good afternoon, Your Honors. Andre Iancu, on
12 behalf of Security First. I will address the Orsini grounds. And just as a
13 reminder, with respect to the Tajima grounds, to Your Honor's question, our
14 colleague, Ms. Sanders, will address that.
15 JUDGE GIANNETTI: Okay. Thank you.
16 MR. IANCU: And in the interest of time, I will make only a few
17 points and obviously answer any questions Your Honors might have. But
18 only a few points with respect to the Orsini, in light of Google's Counsel's
19 comments a bit earlier in the hearing.
20 So let's start by looking at Slide 132. And the fundamental point is
21 that the Orsini reference, which is a very different type of security, of data
22 security, than the claims at issue in the patents before the Board. So just to
23 review, to put things in context, there are multiple steps in the Orsini
24 reference, and they're not the same overall with what we have in the '854 and
25 '609 patents.

1 So specifically, we begin in Orsini with encrypting the whole data
2 set. We begin there. So we first encrypt the whole data set. That's different
3 in and of itself already from what we see in the patents before the Board.
4 Then after that, then we split the encrypted data set into a bunch of shares
5 using a master session key.
6 We also split the master session key itself. And then we put those
7 things together, right, the shares together with the split -- so the split data
8 with the split session key. Okay. And then we again encrypt the data.
9 So now we encrypt each share -- and by the way, we also
10 encrypted this point each piece of the session key. We encrypt all that with
11 different share keys. So already we see in this scheme that we encrypt the
12 data twice. And we've encrypted the master share key once.
13 And then finally, in Orsini, we have an obfuscation step where we
14 mix the now twice encrypted data shares with different share keys. And by
15 the way, we store them on different storage devices. Okay. So that is
16 already -- that whole scheme is quite different from what we see in the
17 patents before the Board.
18 And let's just go to Slide 137. The '609 and '854 patents, you
19 know, they share a common reference, a common specification and, as I
20 said, a very different scheme all together.
21 Slide 138, they add -- even though we have overlapping inventors
22 between the two, many of the same inventive team, but they now add 18
23 new columns of text and 17 new figures, including the key issues that are in
24 the claims at issue here. And the additions are simply not to be found in
25 Orsini.

1 And if we go to the next slide, Slide 139, in the claim, what's
2 reflected as one of the main additions -- what is an example -- is that there is
3 an additional encryption operation to further secure the data chunk not in
4 Orsini. Okay. However, to emphasize, the whole scheme is different. And
5 in Orsini, we have no external key, no encryption to further secure the data,
6 and no encryption in Orsini of the share key.
7 Okay. So that's just the background. So now, if we jump to Slide
8 144, what does Petitioner argue? Petitioner says never mind all those
9 differences, it would simply be obvious to modify the Orsini scheme
10 basically, as shown in Figure 21 -- to add just in encryption step, one more,
11 to encrypt the share keys with a key encryption key to avoid what they call a
12 potential security risk.
13 Okay. But why? Why would it be obvious? First of all, these
14 inventors didn't do it. And a lot of them are in the, you know, the -- and
15 presumptively, they're ones of skill in the art. Obviously, they were working
16 on this exact type of technology, but they didn't think of it originally. They
17 thought of another encryption scheme, but not the ones at the patent -- in the
18 patents at issue.
19 So why? Why would it be obvious to, on top of all the other
20 security measures outlined in Figure 21 of Orsini, why add this other one?
21 And not just that, how precisely to add the additional encryption key. And
22 they say, well, you know, it would be obvious. It was just common
23 knowledge to use the key encryption keys.
24 But to be clear, there's nothing in the record, nowhere, the concept
25 or the suggestion, and I'll get to this in more detail in a second, that a key

1 encryption key or any security measure should be taken in addition to all the
2 other ones to encrypt the share keys.
3 Okay. So now, let's dive into some of this in a bit more detail.
4 Slide 149, please. So now they're trying to answer why would we do this.
5 Why is it -- why would it be obvious? Why should one of skilled in the art
6 add the additional encryption key? And we see the Petitioner's argument on
7 the left of Slide 149. Effectively, they say, "Orsini's obfuscation provides
8 negligible non-cryptographic security," and so on.
9 But what is the evidence? Let's look at Orsini itself. The evidence
10 is detailed that Orsini believed -- and it's highlighted at the bottom of
11 paragraph 380 from Orsini. And I'll quote that highlighted sentence, "When
12 combined, the entire process for securing in data, according to the methods
13 described herein, becomes a comprehensive package for data security."
14 And if we go to Slide 151, we can get into some details about why
15 that is. So we see all from Orsini itself as an explanation as to why they had
16 their own earlier encryption scheme and not the modified encryption scheme
17 that Petitioner would like it to have. So first, it says in paragraph 299 from
18 Orsini, "Then store the encryption keys in different locations from the
19 encrypted data portions or share."
20 Paragraph 379, "One advantage is that it's the security gained from
21 moving shares of the data to different locations on one or more data
22 depositories or storage devices that may be in different logical, physical, or
23 geographical locations." And paragraph 353 again, "The key required to
24 decrypt the share is stored in a different data (INDISCERNIBLE)."
25 And so bottom line is not only are you obfuscating, you're storing

1 them in different locations. And as a reminder, all of this in Orsini is after
2 the data itself -- which is ultimately the purpose of securing here -- is already
3 encrypted not once but twice. Once with a share key, which with a -- I'm
4 sorry, with a master sessions key, which itself is being split and encrypted,
5 and the second time with a share key. All of this in the original Orsini
6 scheme. So why would we have a different one?
7 Let's look at Slide 152, next slide. And the experts agree that
8 storing chunks separately adds a high level of security. On the left of Slide
9 152, we see the deposition testimony of Dr. Bhattacharjee, Petitioner's
10 expert, where he says, "It's nearly perfect security because no matter how
11 much computation they have, they're not going to be able to get to it. So it's
12 a very secure method." This obfuscation method and storing separately.
13 And then our experts, Dr. Rubin, agrees, as we see also on Slide 152.
14 Next, Slide 153. Again, from Orsini itself, that's -- the possibility
15 of compromising the data is greatly reduced and security is gained from
16 storing the data chunks separately and the keys separately.
17 And then finally, Slide 154, other references that are in the record,
18 the Petitioner itself has put in the record, generally agree. And here's an
19 example from the Hayhurst reference where they say in paragraph 8 of
20 Hayhurst, "The segmented and distributed storage of the media file provides
21 a high level of security."
22 So for all of the hypothetical, generic arguments that are being
23 made that, sure, more security is better than less security, there is no
24 demonstration that there's a motivation in Orsini to be modified to change
25 the security mechanism. And frankly, there is nothing, no explanation as to

1 whether in fact the addition of an additional security encryption scheme,
2 after all the steps already taken, would actually increase security. That is not
3 a given at all.
4 This is a complex art. Encryption is very complicated. And the
5 second you add another encryption step, such as with an external key
6 encryption key, you need to worry about managing it. You need to worry
7 about making sure that it is also safely secured and that it does not somehow
8 compromise the security of the other steps, whether it's an obfuscation step
9 or another encryption step.
10 JUDGE BELISLE: So Counsel, this is Judge Belisle. All of what
11 you said is what bugs me about this obviousness sort of case on this
12 particular reference. And has either expert made any statement as to what is
13 involved with -- as what Petitioner would say just encrypting it again using
14 this well-known key encryption key? Do you have anything from any --
15 from either expert that sheds some light on whether that really is a simple
16 thing?
17 I mean, I understand from the Orsini reference to the challenge
18 patent that there was a significant amount of disclosure that was added with
19 a lot of drawings to get it from its original disclosure to the -- well, what is
20 claimed now. So all the way around, is there anything from the experts on
21 this particular point about adding that additional level of encryption?
22 MR. IANCU: Well, there is at least evidence from Dr. Rubin,
23 SFI's expert, Patent Owner's expert. And he explains that this is a
24 complicated art. And for example, if we look at Dr. Rubin's paragraph 66,
25 the Rubin declaration, there's a fairly lengthy explanation as to why adding,

1 you know, all these additional steps or even one additional step has to be
2 very carefully done. And it can actually in fact compromise the security.
3 And also in the record, if we can go to -- what slide is --
4 MR. LOWENSTEIN: 161.
5 MR. IANCU: 161. We see it already on the screen. We already
6 have -- we have put on the record the fact that it's generally known, this is
7 one of the more important cryptography volumes out there, that key
8 management is the hardest part of cryptography. And keeping the key secret
9 is very difficult.
10 So I think there is, Your Honor, plenty of statements in the record
11 from our side that you just can't do it. And I don't think that there is
12 anything in the record from Petitioner to explain how exactly they propose
13 to add the key encryption key step at the end of Figure 21 in Orsini. How do
14 you apply it precisely? And then most importantly, what do you do with it?
15 How do you manage it? Where do you put it?
16 At some point, you have to manage that. And then what, do they
17 suggest should we then encrypt that key encryption key too with another
18 key? It's just -- you know, it's a different scheme, that's the main point.
19 And, you know, whatever one thinks of the Orsini scheme, it's a complete
20 scheme. They thought it was very secure. And the patents, though, come up
21 with a different, quite innovative new scheme.
22 Okay. So unless there's anything else on that, I want to make one
23 last -- a point about Petitioner's argument with respect to Orsini. And if we
24 can go, please, to the Petitioner's slides. And let's look at Slide 140, which I
25 think Petitioner's Counsel used a bit earlier in the hearing.

1 And, you know, they say a person of ordinary skill knows about
2 key encryption keys. And they argue it was conventional to use it and
3 therefore should just simply be applied to the Orsini scheme of Figure 21.
4 And they give these three examples from -- I'm sorry, these two examples
5 from the record, from the prior art.
6 And Counsel, earlier today, spoke about example 1036. And it
7 says, well, look, in example 1036, you know, it says that security can be
8 done by encrypting the encryption keys, with a key encryption key,
9 highlighted by them in red. But it's not all the time. Look at the quote itself,
10 look at the beginning.
11 And Colette, I don't know if you can highlight. Are you able to or
12 no?
13 MR. LOWENSTEIN: Yeah, she's highlighting.
14 MR. IANCU: Oh, okay. So at the very top, security for such a
15 system where the encryption keys are included with the encrypted message,
16 that is not what's happening in Orsini. Orsini figured out a different scheme.
17 In Orsini, Figure 21, we are obfuscating. We are not storing the encryption
18 keys with the encrypted message, we're mixing and matching, and then we're
19 also distributing all over into different storage devices. So that's not
20 applicable.
21 Let's look at the example they give in 1035. And they highlight
22 there in 1035 that cryptographic keys should never -- and Counsel
23 emphasized the word never -- never occur in clear form outside the -- in
24 cryptographic device. But Counsel skipped the exception, which is right
25 after, except under secure conditions during the period when keys are

1 originally distributed and installed or when stored in a secure place such as a
2 safe. So already we see that if we have a different way of securing the
3 encryption keys, then this example here does not apply.
4 So with that, Your Honors, unless -- well, let me pause and see if
5 there are any questions. But otherwise, I will cede the rest of my time to my
6 colleague to talk about the Tajima.
7 JUDGE BELISLE: None for me.
8 MR. IANCU: Okay. Thank you all very much.
9 JUDGE GIANNETTI: All right. Thank you, Counsel. Now, we
10 have Ms. Sanders.
11 MS. SANDERS: Good afternoon, Your Honors. My name is
12 Haley Sanders for the Patent Owner, Security First Innovations. And today,
13 I'll be talking about the '116 patent, specifically the Tajima Grounds. And in
14 the interest of time, I'll be focusing on Petitioner's Ground 2, Tajima-Foster;
15 and Ground 3, Tajima-Rivest.
16 Ground 5, Foster-Hayhurst should be rejected by the Board for the
17 reasons already discussed by my colleague, Mr. Lowenstein. And for
18 Grounds 1 and 4, Patent Owner rests on its arguments and its briefing. But I
19 would like to note that should the Board reject Ground 3's combination of
20 Tajima-Rivest, Ground 4, Tajima-Rivest-Shyu would necessarily fail as
21 well.
22 And I won't spend too much time on this. But again, we would
23 object to the improperly incorporated by reference expert replied declaration
24 as well as the newly introduced exhibits.
25 And so just as a quick background of the independent claims at

1 issue here, Claim 1 on Slide 172, requires chunking, encrypting, and
2 obfuscating the encryption keys. And so the method splits the data set into
3 chunks, encrypts each one of those chunks with the distinct encryption key,
4 obfuscates those encryption keys, and then stores each chunk with a
5 different obfuscated key across different storage devices. And obfuscation
6 can be broader, but it does include storing data with a key that can't decrypt
7 it.
8 Claim 9, shown here on Slide 173, performs the same steps as
9 Claim 1, with the important distinction that it transforms rather than
10 obfuscates the encryption key. This transformation includes all-or-nothing
11 transformation as well as other data transformation such as encryption. And
12 just -- I also wanted to note very quickly that earlier today, Petitioner
13 conceded that Orsini is not prior art to the '116.
14 So moving on to Petitioner's Ground 2, Tajima-Foster. On Slide
15 175 are the three main reasons why a POSITA would not be motivated to
16 combine Tajima with Foster: first, Tajima and Foster solve different
17 problems in different fields; second, they're fundamentally incompatible
18 with one another; and third, Petitioner's combination is redundant because
19 Tajima already solves the problem Petitioner proposes to address by adding
20 Foster.
21 And the standard here that Petitioner must meet is whether a
22 POSITA would have selected and combined the prior art elements in the
23 normal course of research and development. And what that means here is
24 whether a POSITA would have been motivated in trying to improve Tajima,
25 would they have looked to it such a disparate reference such as Foster and

1 selected it to combine that with Tajima?
2 And again, I'll move through this rather quickly. But Tajima and
3 Foster are -- solve different problems, and they're from different fields. So
4 Tajima secures storage of personal information. And Foster, as my
5 colleague Mr. Lowenstein has explained, improves random access to a
6 media stream. It has nothing to do with personal information or secure data
7 storage. And --
8 JUDGE KAZHDAN: Just a quick question.
9 MS. SANDERS: Yes?
10 JUDGE KAZHDAN: I thought there was an obviousness ground
11 based on Tajima alone, which -- as understood by the art reference. I
12 didn't -- are we going to talk about that also or --
13 MS. SANDERS: We rest on our arguments in our briefing. I'm
14 just going to talk about Grounds 2 and 3, which are Tajima-Foster and
15 Tajima-Rivest.
16 MR. IANCU: Ask him if he has a question.
17 MS. SANDERS: Do you have a specific question about the
18 Tajima alone?
19 JUDGE KAZHDAN: Well, it's just -- yeah, we're good there.
20 Thank you.
21 MS. SANDERS: Thank you, Your Honor. So Tajima and Foster
22 address different issues seen in different prior art. And Tajima addresses,
23 again, the risk of security issues with data registered to one specific area.
24 And the risk there is that the information can be viewed by an unauthorized
25 user because it's all stored in one location.

1 And Foster seeks to improve upon the prior art to reduce latencies
2 and allow for random access of content. And they're achieving different
3 goals, but they do both have to confront a similar problem, what to do with
4 key information. But because of the different contexts in which these
5 references arise, they do solve them differently.
6 So Tajima solves the issue in its prior art by separating the key
7 information and the corresponding encrypted data and storing them under
8 separate control. Foster, on the other hand, has to transport the key with the
9 data packet it encrypts. So Foster has to encrypt the packet keys.
10 The second reason why the Board should reject this combination is
11 that Tajima and Foster are fundamentally incompatible with one another.
12 And the bottom line, as we've said, that Foster's whole invention is
13 synchronized transmission, keeping the key with the data it encrypts. And I
14 apologize, I haven't been announcing the slide numbers. This is Slide 179.
15 And on Slide 180, you can see that the fundamental -- at the core
16 of Tajima is the complete opposite, that you have to keep the key
17 information separate from the data chunk that encrypts.
18 And Slide 181, Foster discourages this combination, again,
19 because it --
20 JUDGE GIANNETTI: So Counsel, are you going to raise the
21 issue of the key information, whether it includes the key or not, or is that --
22 MS. SANDERS: No. I'm not addressing that today. We rest on
23 our --
24 JUDGE GIANNETTI: Okay.
25 MS SANDERS: -- arguments in the briefing, just for the sake of

1 time.
2 JUDGE GIANNETTI: But you're not conceding that argument?
3 MS. SANDERS: No, we are not.
4 JUDGE GIANNETTI: All right. Okay. Thank you.
5 MS. SANDERS: Mm-hmm. So Foster discourages this
6 combination because it requires the key information to be kept with the data
7 packet. And, you know, Tajima says the exact opposite, you have to keep
8 the key information and the data chunks separate.
9 Tajima is an alternative to be used where key encryption is not
10 secure. Tajima recognizes that even if you were to use encryption, a danger
11 still remains that given enough time, a high-speed computer, a sophisticated
12 attacker can decrypt the encrypted personal information. So it avoids
13 encryption. It saw a security issue, and it avoids that issue by separating the
14 key information from the data it encrypts, storing it in different locations and
15 under separate control.
16 So just to summarize -- and I want to point out Slide 183, there's a
17 slight error on this slide. The bottom right, most cells should say that Foster
18 secures the key information through encryption. So just overall, these
19 references are so different. They have different focuses, they arise in
20 different contexts, and they solve different goals. And it's just a POSITA
21 would not have selected these two disparate references in the normal course
22 of research and development to yield this combination.
23 And if you'll all excuse me, I'll grab water here real quick. And so
24 the final reason I want us to touch on as to why this combination fails is that
25 it is redundant. So as I said earlier, in serving these two different goals,

1 Foster and Tajima confront a similar issue of what to do with securing plain
2 text key information. And they solve this in very different ways, though.
3 And again, the combination here that Petitioner proposes is for a
4 single reason of increasing security in a single scenario where an attacker
5 would gain access to all of Tajima's data fragments. And this is the only
6 reason they provide that would motivate this combination. But Tajima
7 already solves this problem. It recognized this problem in the prior art and
8 solved this issue.
9 And on Slide 185, again, these references are addressing a similar
10 issue of what to do with securing plain text key information, but they
11 accomplish that differently. Tajima stores key information with an unrelated
12 data portion in areas under separate control, which is very different from
13 what Foster does which is to encrypt the key information.
14 JUDGE KAZHDAN: What's your response to Petitioner's point
15 about it's like having a lock and an alarm system, so maybe two is better
16 than one?
17 MS. SANDERS: Yes. So yes, it's true that adding more layers of
18 security would -- or adding more layers of encryption would add more
19 security. But Petitioner fails to weigh the drawbacks of that system. The
20 more complex you make a cryptographic system, the more issues there are to
21 manage, and there's more room for error. And that can actually introduce a
22 larger risk of security issues.
23 And further, Petitioner stated that it recognized in every scenario
24 that complexity is an issue that a POSITA must address. And they didn't
25 address this in their briefing, what the specific drawback would be. So --

1 JUDGE KAZHDAN: I'm sorry, but -- so, like, this just seems like
2 we're talking about benefits and drawbacks. And your point is there are
3 drawbacks. And their point is there are benefits. But I think they've said
4 some case law that, you know, that's standard and you don't -- it's not -- it
5 can be obvious despite the fact that you get some drawbacks because you get
6 some benefits and sort of -- you know, that trade-off is one that we often
7 make in different facets.
8 MS. SANDERES: Of course. So --
9 MR. LOWENSTEIN: One second -- take a second -- say one
10 second --
11 MS. SANDERS: If you'll give me one moment to confirm with
12 my colleagues. Thank you.
13 JUDGE KAZHDAN: Just because we have a little pause there, let
14 me flag for you. You have, like, 45 minutes left. So 15 minutes until you're
15 in rebuttal. But I'm not rushing you at all.
16 MS. SANDERS: Okay. So yes, we're weighing the benefits and
17 the drawbacks. But really, the point here is that Tajima has already solved
18 this issue. And -- apologies, one moment. So Tajima addresses this issue
19 already. It does not need Foster's further encryption. We don't have to
20 further complicate the system because Tajima takes the data and the key --
21 corresponding key information and puts it under separate control in separate
22 locations.
23 JUDGE GIANNETTI: This is Judge Giannetti. Just to follow up
24 on Judge Kazhdan's argument, it's just taking your argument to its logical
25 conclusion that it's added complexity. I mean, isn't that true anytime you

1 add additional levels of security it's going to be more complex, there are
2 going to be more keys to manage, more levels of security to manage it?
3 If we were to follow your logic, there would never be any
4 patentable improvements in security systems because they would all lead to
5 more complexity.
6 MS. SANDERS: Of course. So the added complexity is not
7 always fatal to the combination. But here, when we're weighing it against
8 the benefits of how Tajima was already designed and the fact that it already
9 addressed this particular issue, the -- after weighing that, the outcome is that
10 it just would not have provided enough of a motivation to combine.
11 JUDGE GIANNETTI: All right. Thank you.
12 MS. SANDERS: And Petitioner did not prove that, did not show
13 that the benefits outweighed the drawbacks that come with complexity.
14 JUDGE GIANNETTI: Well, wasn't there expert testimony to that
15 effect? I mean, how much -- what would you require, test the data or
16 something? It seems they probably have expert testimony on this point.
17 MS. SANDERS: They did. But I don't believe in their briefing
18 they really addressed the drawbacks.
19 JUDGE GIANNETTI: I see. Well, maybe we'll --
20 MS. SANDERS: Yeah.
21 JUDGE GIANNETTI: Well, maybe our -- the Petitioner will give
22 us some help on surrebuttal.
23 MS. SANDERS: And I will also say that the benefit that they
24 touted was just some vague increased level of security.
25 JUDGE GIANNETTI: I see.

1 MS. SANDERS: So I don't think it was of enough detail to justify
2 the added complexity and risks that come with further encryption.
3 JUDGE BELISLE: Well, Counsel, this is Judge Belisle. If we
4 agreed that there is a reason to combine the references, the skilled artisan
5 would have had a reason to combine those references, does the combination
6 of those -- do you -- is there any disagreement that the combination of those
7 references would teach the limitations of the claim as claimed so be it not,
8 perhaps, disclosures in various references but what's claimed?
9 MS. SANDERS: Excuse me, one moment. So with respect to this
10 particular ground, we are not arguing that it does not meet a claim limitation.
11 We're arguing just the motivation to combine.
12 JUDGE BELISLE: Okay. I understand. Thank you.
13 MS. SANDERS: Okay.
14 JUDGE GIANNETTI: Thank you.
15 MS. SANDERS: And just to circle back to why Tajima has
16 adequate security and already addresses Petitioner's motivation is this -- the
17 key is the separate control. And that's critical here because it prevents an
18 attacker from getting all of the keys and all of the corresponding data.
19 And when I say separate control, I mean things like different
20 employees, different levels of access, different security policies, firewalls.
21 And that means a single insider can't get access to the data or a single hacker
22 just by getting through a single firewall. All they would be able to get is one
23 single data fragment and unrelated key information, which is completely
24 useless to them.
25 And let me see where I'm at. And this is shown in Slide 186

1 through the use -- and Tajima's Figure 5, these separate secured -- or
2 certificate authorities. That would be one example of separate control. And
3 Tajima states explicitly the personal information cannot be viewed unless all
4 of the areas in which data are registered are exposed. And so that's the key
5 to how Tajima protects the personal information and already solves this
6 problem that Petitioner says would motivate the combination.
7 And I will skip ahead. And again, so Tajima solves the problem
8 that Petitioner puts forward that would motivate the combination. And
9 Petitioner's expert admits that it addresses this particular vulnerability. And
10 this is on Slide 189.
11 And so when you have separate control, data, and key information
12 on different databases belonging to separate service sites, according to Dr.
13 Bhattacharjee, "An attacker that successfully gained unauthorized access to a
14 service site could procure only a single unintelligible data fragment and the
15 attacker would not be able to recover the user's personal information."
16 And so here, as a matter of law, Petitioner is failing to provide a
17 specific explanation why Tajima did not already accomplish this increased
18 level of security that allegedly motivates this combination. Because Tajima
19 was already concerned with preventing the access to all of the data
20 fragments and accomplished that.
21 And further, as we mentioned earlier, Tajima -- the design in
22 Tajima is nearly perfect security. The separate control in separate areas is
23 nearly perfect, according to Petitioner's expert, Dr. Bhattacharjee. And so
24 because Tajima addresses this issue and its nearly perfect security, there's no
25 reason why a POSITA would look to improve upon it, with Foster's key

1 encryption keys further complicating the system without really any benefit
2 that would outweigh the risks.
3 And I thought of an analogy for this. So it's raining, you get an
4 umbrella that it keeps you plenty dry. You could get another umbrella and
5 that would keep your first umbrella dry and so on and so forth. And of
6 course, it would provide more protection. But at the end of the day, that
7 original umbrella kept you plenty dry.
8 And just like adding more levels of encryption, Petitioner's --
9 counsel for Petitioner mentioned earlier that as you're adding this key
10 encryption key scheme, that would end up with millions and millions of keys
11 that you would have to manage and keep track of. So I guess the analogy
12 would be you have too many umbrellas to hold and you have too many keys
13 to manage, and that would outweigh any benefits that a Petitioner puts
14 forward for this combination.
15 And additionally, you have too many umbrellas, to continue with
16 this analogy, and before you know it the wind is blowing and your umbrellas
17 are colliding. And in the same way that further complexity can introduce
18 errors and security issues, the more umbrellas, it might defeat the purpose of
19 the umbrellas in the first place. Thank you for bearing with me in that
20 analogy.
21 And unless there's any more questions on this Tajima-Foster
22 Ground, I can move on to Petitioner's Ground 3, Tajima-Rivest.
23 JUDGE GIANNETTI: Nothing from me. I think you can move
24 on, Counsel.
25 MS. SANDERS: Okay. Great. Thank you, Your Honor. So Slide

1 191 -- I'll move on to Ground 3, Tajima-Rivest. And on Slide 192, again, I
2 have three main reasons why a POSITA would not be motivated to combine
3 these references: first, again, just like with Tajima-Foster, this combination
4 is redundant; and second, Rivest's all-or-nothing transformation does not
5 actually provide any additional security and violates Kerckhoffs' principle;
6 and third, this combination actually creates data integrity problems.
7 And Slide 192, just as a small background, Rivest is just a pre-
8 processing step, that standing alone does not provide adequate protection to
9 a data set. So this all-or-nothing transformation masks the data set in a way
10 that would force an attacker to decrypt the entire data set before it can make
11 sense of any single piece of a data set.
12 But if it's used without further steps, such as further encryption or
13 splitting, anyone who knows the random number that was used to perform
14 the transformation can invert this transformation to obtain the original data
15 set.
16 And so Slide 194, so this shows Petitioner's combination. And it's
17 using Rivest in the same manner that it did Foster in its Tajima-Foster
18 combination, which is to protect the plain text key information. But Rivest
19 here is even further afield than Foster. At least Foster mentions the
20 protection of key information, but Rivest says nothing about keys or key
21 information.
22 And again, as I've said many times, Tajima already solves this
23 problem of securing plain text key information. It already solves the only
24 issue that Petitioner says would motivate the combination. And so I -- a
25 POSTIA would just not have recognized -- would not have been motivated

1 to combine because it would have recognized the security of Tajima as
2 sufficient for this specific goal and scenario that Petitioner says would
3 motivate this combination.
4 And so on Slide 195, Petitioner proposes to use a public key as the
5 all-or-nothing transformation number. But by definition, public keys are
6 known to the public. So this public AoNT number cannot possibly provide
7 security.
8 And you heard in Petitioner's briefing and its demonstratives, the
9 Petitioner stated that the use of a public key and the fact that all-or-nothing
10 transformation and this combination would be kept secret, this still does not
11 add any more security. Because even though this is kept secret, it's still
12 relying on the secrecy of the algorithm. And a brute force attacker could
13 simply try all of the limited number of all-or-nothing transformations to
14 access the key information because this key is public.
15 Am I out of focus again? And Slide 196, because the key is public,
16 because this all-or-nothing transformation is public, this violates one of the
17 more basic rules of cryptography, Kerckhoffs' principle, which requires the
18 security of encrypted content rely on the secrecy of the key.
19 And its briefing, Petitioner argued that Kerckhoffs' principle is just
20 a guideline. But again, that's removing this principle from context and
21 asking you to believe that a POSITA would have known this principle that's
22 taught to every beginning cryptographer and just simply ignored its
23 reasoning.
24 The only way this combination would provide further security --
25 and I'm on Slide 197 now -- is if further steps were performed, such as

1 further encryption or fragmentation of the key information. And that's just
2 not disclosed in the combination nor by Tajima. So without these steps,
3 there's no further security and this combination does not provide any more
4 security to Tajima.
5 And lastly, the last thing I want to touch on here on Slide 198 is
6 that this particular combination actually creates the risk of data loss. And
7 Rivest explicitly says that it's all-or-nothing encryption -- all-or-nothing
8 transformation, excuse me, has terrible error propagation properties in that --
9 and in this combination, if any single block of the transformed key
10 information is damaged, it's likely that every message block will be
11 damaged.
12 And so what you're left with is an entire key information that's
13 damaged and a data fragment that you can never access. And so in order to
14 avoid this, Rivest teaches that you need to use reliable transmission means.
15 But Petitioner's combination does not use reliable transmission means. It did
16 argue that its combination only stores this transformed key information with
17 the data fragments.
18 But in its reply, it did admit that individual transformed message
19 blocks are kept and transmitted together. So this combination does not use
20 these reliable transmission means and it creates the risk for data loss. And a
21 POSITA would not be motivated to create this combination because, again,
22 weighing the benefits and the drawbacks, it just would not provide the
23 motivation to combine.
24 And that is all I have. So just in sum, Tajima -- Petitioner puts
25 forward, again, one specific reason, an increased level of security which is

1 very vague in a specific scenario, which is where all of Tajima's data
2 fragments would be accessed. But Tajima recognized that issue in the prior
3 art, and it proceeded to solve it.
4 And as Petitioner's expert states, the scheme of Tajima provides
5 nearly perfect security. So it addresses this issue, provides nearly perfect
6 security. And there's just no reason, when looking at the drawbacks, why a
7 POSITA would be motivated to combine Tajima with Foster or Tajima with
8 Rivest.
9 And unless there's any questions, I am finished.
10 JUDGE GIANNETTI: Anything from the panel? All right.
11 Thank you very --
12 JUDGE KAZHDAN: You have 16 minutes for your rebuttal.
13 MS. SANDERS: We have that extra 15 minutes.
14 JUDGE GIANNETTI: Yes. They have the extra 15 minutes,
15 Counsel. So I think they have more than that, right? Yes, I think they
16 have -- well --
17 JUDGE KAZHDAN: I'm sorry, I didn't mean 16, I meant 46. I
18 miscounted. My bad.
19 MS. SANDERS: We have 46?
20 JUDGE KAZHDAN: No, 31. There we go.
21 JUDGE GIANNETTI: Yesh, 31. That's more like it. Okay. So
22 you have 30 -- you have a couple extra minutes on top of your 31. And what
23 is it -- so for the rebuttal, it's 20 minutes for rebuttal? They have 20 minutes
24 left, Counsel?
25 JUDGE KAZHDAN: Petitioner has --

1 JUDGE GIANNETTI: Petitioner has --
2 JUDGE KAZHDAN: -- 15.
3 JUDGE GIANNETTI: -- 15. Okay. All right.
4 MS. SANDERS: Okay. Thank you, Your Honor.
5 MR. NIEBERG: Could we take -- oh, I'm sorry.
6 JUDGE GIANNETTI: Yes, go ahead.
7 MR. NIEBERG: I was going to ask if we could take a short break,
8 a restroom break.
9 JUDGE GIANNETTI: All right. Yes. Let's take a quick break.
10 Let's try to do it in 10 minutes, quickly, okay?
11 (Whereupon, the above-entitled matter went off the record at 4:50
12 p.m. and resumed at 4:59 p.m.)
13 JUDGE GIANNETTI: All right. I think we're ready to proceed.
14 My timekeepers tell me that, Petitioner, you have 15 minutes for your
15 rebuttal. I remind you that your rebuttal is limited to points that were raised
16 by the Patent Owner in their case.
17 MR. NIEBERG: Okay. Thank you, Your Honors.
18 JUDGE GIANNETTI: All right.
19 MR. NIEBERG: So I'd like to start with a point that was raised a
20 few times by SFI's Counsel alleging that Dr. Bhattacharjee admitted that
21 Tajima and Orsini had perfect security and they put up some deposition
22 testimony. Can you please turn to their Slide 190?
23 If you look on the left, the testimony that they quote from Dr.
24 Bhattacharjee's deposition, he said -- and they -- so they take out of context,
25 he says "in nearly perfect security." But look at what he's talking about

1 before that. He's talking about taking a piece of data on, like, a USB drive
2 and removing it from a network, taking it offline. So he said if you take the
3 data and storage space and remove it from a network, then you can't have a
4 network-based attack. So in that case, you have perfect security.
5 But he never testified that Orsini or Tajima have perfect security.
6 He just said that if you took their systems offline, you'd have perfect
7 security. But Orsini's and Tajima's databases, storage places, they're online.
8 They're subject to online attacks. That's why the security comes -- there's
9 added security from using a key encryption key, for example.
10 So there were questions and allegations that Dr. Bhattacharjee
11 didn't address the alleged downsides of key management for using a key
12 encryption key in Tajima-Foster and Orsini Grounds. He did. So for
13 Tajima-Foster, for example, in his initial declaration, Exhibit 1003 in the
14 '116 matter, at paragraphs 157 to 159, which were cited in our petition of
15 pages 38 to 40, Dr. Bhattacharjee discussed the benefits of using a key
16 encryption key to encrypt keys like Tajima.
17 In our '116 petition of pages 39 to 40, we argued that a POSA
18 would have had a reasonable expectation in success because it's a
19 straightforward modification requiring only conventional and routine skill
20 for a POSA. And we argued that it would impose little additional burden to
21 have this one additional well-known conventional key, and we cited Dr.
22 Bhattacharjee's expert testimony in support of that. That's at Exhibit 1003,
23 paragraphs 161 to 162.
24 JUDGE BELISLE: So Counsel, it's Judge Belisle. On that point,
25 other than repeating what you just said to us by your expert, what does your

1 expert say for why or why not that that is just -- you can just do it, like
2 there's no big deal just adding this additional key encryption to a reference
3 that didn't have it.
4 MR. NIEBERG: Okay. So I'm going to switch to the -- I was just
5 looking for a citation for that. So in '854, for example, so if you look to page
6 27 of our petition, we cited Dr. Bhattacharjee's paragraphs 96 to 97, and we
7 quoted Exhibit 1022 which corroborated that a POSA's background
8 knowledge included storing keys in a centralized location that is itself is
9 secure from access by attacker.
10 So there are questions that talks about, well, how do you secure the
11 key encryption key? That's what we explained in our petition of page 27
12 with corroborating evidence and support from our expert that the storing
13 keys in secure locations was known. That's where the key encryption key
14 would be in a secured location.
15 And so what's happening here is you have data chunks and its keys
16 are being sent to some storage device away from the system. And that key
17 in our obvious modification is encrypted with a key encryption key. And the
18 key encryption key is kept back in a secured storage location, a well-known
19 key store. And so what that does is even if an attacker gets to the data that's
20 outside the system, they would still have to get into your system and break
21 into your key store for a key encryption key. And that's the whole point of
22 using the key encryption key is because that's an additional level of security
23 that some -- an attacker would have to get through to get to your data.
24 And then so in paragraph -- getting into the '854 matter, it's the
25 patent matter. In Dr. Bhattacharjee, paragraph 133, which we cited on pages

1 43 through 44 of our petition, Dr. Bhattacharjee testified that a POSA would
2 have managed the key encryption key in an external storage system for the
3 reasons discussed above in his section 1A. That's the paragraph 96 to 97
4 that I just discussed where it was known how to store keys, keep them in a
5 secure location.
6 And so he's explaining that in his obvious modification, the key
7 encryption keys would be stored using the conventional, well-known
8 techniques of storing keys, like key encryption key. And to the point of
9 complexity of adding a key encryption key, you can search in vain in their
10 patents for teachings about additional key management or about there being
11 alleged problems using a key encryption key.
12 Their patent expressly relies on existing key encryption key
13 technology and existing key standards, existing key management. And
14 there's -- they don't allege there are any problems with key management.
15 They don't allege there are any problems with key encryption key, key
16 management. They teach nothing about how to further secure -- how to
17 store key encryption key.
18 SFI's Counsel pointed to all the new disclosures they have in the
19 '854 patent of Orsini. There's nothing there that talks about the problems or
20 the details or even suggests there's a problem or suggests details of key
21 management for key encryption key. And that's for good reason, it was
22 well-known. It was simple for a person of skill.
23 There was arguments about how --
24 JUDGE BELISLE: Counsel, maybe we can just do a bit more on
25 that point.

1 MR. NIEBERG: Yeah.
2 JUDGE BELISLE: My concern isn't whether it was known to use
3 a key encrypting key to encrypt keys. I think, perhaps, everyone agrees that
4 that is known, it's shown in literature that encrypting these keys is a known
5 thing particularly amongst the skilled artisans.
6 But the issue is whether --- just even with that knowledge, what
7 would it have taken to modify what's disclosed in the reference to achieve
8 that additional encryption? What I'm hearing from Petitioner is that, oh, you
9 just do it. You would just do it and it'd work out fine.
10 And what I'm hearing from Patent Owner is, wait a minute, you
11 can't just do it. The whole thing has to be interwoven into how the system is
12 managing keys and it's more complicated than that. But I don't have a whole
13 lot of evidence one way or the other as to which way to lean on that when it
14 comes to how the skilled artisan would view that.
15 And sorry for my voice. I went to bed fine, and I woke up like
16 this, so.
17 MR. NIEBERG: It's been a long day. So I think one of the best
18 places to look, as I said, is, like, page 27 of our '854 petition where we cited
19 Dr. Bhattacharjee's paragraph 96 to 97. And our petition itself quoted
20 Exhibit 1022 that talks about how it was well-known to have systems for
21 storing and managing keys.
22 And the point being that -- further to that point is that, as you just
23 said, we all acknowledge that key encryption keys were known and used. A
24 corollary to that is the management of those keys, how to use them, how to
25 manage them -- was also well-known and understood by a POSA. That

1 problem had already been solved.
2 And their patents don't purport to have added anything to that
3 aspect of it. They're relying on existing technologies. They're relying on
4 existing key encryption standards called AES and DES, which as we cited in
5 our reply -- and I apologize, I don't have the exhibits at hand. I could get
6 them for you momentarily. We cited where those encryption standards
7 themselves taught key management and using key encryption keys.
8 So the same basic prior art standards, that their patents rely on as
9 support for using a key encryption key taught, how to manage those keys. It
10 was already solved in the art. Again, like I said, we've cited evidence of
11 that, of where this key management problem -- to extent it's a problem --
12 was addressed and well-known. And now, to the -- did I answer your
13 question? I know it's -- you're -- I want to -- it's an important point.
14 JUDGE BELISLE: I'm going to look at the citations that you
15 provided in that. So that is helpful. And I'll take a look at that.
16 MR. NIEBERG: Thank you. There's also been a little bit talking
17 past each other about whether there would actually be benefits to either -- to
18 encrypting key encryption keys in Tajima-Foster and in the Orsini Grounds.
19 And Counsel for SFI gave an umbrella analogy that, well, you could just
20 keep having a hundred umbrellas. You know, after a while, it gets
21 ridiculous.
22 Well, when I go out in the rain, I take an umbrella. If it's a heavy
23 rain, I'm going to have a rain jacket on. I'm going to put on rain boots.
24 Why? Because they provide different protection. The umbrella prevents the
25 rain from above. My rain boots are going to protect rain that splashes up on

1 me. The same is true in a sense of a key encryption key and obfuscation.
2 So if you could please turn to our Slide 145, Google Slide 145. So
3 there was also an allegation -- a suggestion that we made up this non-
4 cryptographic security for obfuscation. That's SFI's own language.
5 Look to the left of Slide 145. They argued in their POR -- they
6 admitted that in Orsini, it's useless because -- so they say -- I'm sorry, they
7 said that Orsini already uses a non-cryptographic operation that is not based
8 on a key to further secure the data chunks. So they admitted that Orsini uses
9 non-cryptographic obfuscation.
10 Now, look to the right, top right of Slide 145. SFI's expert, Dr.
11 Rubin, admitted that Orsini's non-cryptographic approach, however, cannot
12 protect a data set if an attacker has access to all the shares. He continued,
13 that reconstruction becomes straightforward.
14 Now, look to the bottom right of Slide 145. SFI admits that the
15 key encryption key provides security because it prevents someone with
16 access to all the content from decrypting it. That is our argument for
17 Orsini's obviousness and for the team of Foster. Obfuscation does not
18 protect you when an attacker obtains all of the shares.
19 The key encryption key is what does that. That the risk of the data
20 being obtained was a possibility whenever you have a motivated attacker.
21 There's no such thing as perfect security, that storage devices could break
22 down. And the well-known solution to that problem was the key encryption
23 key, as SFI itself admits that that's the problem that the key encryption key
24 solved.
25 And their patent doesn't tell you that. Why? Because it was

1 known. The protection provided by a key encryption key, the exact
2 protection we argued in our petitions, the exact protection that they admit in
3 their '116 sur-reply was well-known. That's why all the evidence that we
4 cited says you should encrypt keys with key encryption keys. It provides
5 you this extra blanket of security that you're going to want to use.
6 So there's a lot of questions about Foster and the instructions to the
7 storage device. And so I want to take a step back and just recall again how
8 this played out. We submitted our petition and we had an anticipation
9 argument and an obviousness argument for Foster. And in our view, Claim
10 1 of the '609 patent is very broad. And it doesn't require that the processor
11 instruct the storage device.
12 In our view, if you look to the claim -- and more importantly, if
13 you look to their specification and what it actually discloses for the
14 processors and the storage devices -- there's nothing there that suggests that
15 the processor has to instruct the storage device. So we had a good faith,
16 reasonable basis to believe that the -- and we still do -- that the claim is
17 broad and so that's why it fosters anticipation.
18 In our anticipation argument, we believe that Foster anticipates by
19 storing the data in a storage device at a recipient. And I want to point you to
20 our Slide 66, for example, just to put more concreteness on this. So we had
21 an anticipation argument, and it was our view then and it's still our view now
22 that with the -- if box 430 -- that Foster says that that stores data. And we
23 still believe that that meets the claim.
24 However, we also argued an obviousness ground where a person of
25 skill would say, well, Foster has this really good encryption technique that is

1 used for -- that I would understand could be useful for video-on-demand
2 services. And so what would be useful to do is -- and be obvious and
3 motivation is -- you take Foster's encryption technique in a system that's
4 already performing video-on-demand. And then that system, it encrypts it
5 using Foster's technique. And it would be obvious then to store Foster-
6 encrypted data on a storage device coupled to the processor.
7 And the reason for is -- and as I've explained in video-on-demand,
8 the data - encrypted data is stored on a server and then it downloaded to a
9 user, regardless of whether it's streamed, downloaded, movie over live
10 television. It doesn't matter. The data's stored somewhere before it gets
11 transferred to a user.
12 And our obviousness argument was, okay, you would use Foster's
13 encryption technique to store encrypted data on a local storage device, a
14 local server or storage device coupled directly to the processor for video-on-
15 demand purposes. And there's no -- they didn't allege in their POR that that
16 doesn't meet the claims even under their claim construction for -- about
17 instruction. They only attacked the motivation to do it.
18 They did not say if -- they did not argue, well, even if there were
19 motivation, the claim -- your obvious argument failed. What they said is
20 you don't --
21 JUDGE KAZHDAN: Counsel, you're basically out of time. So if
22 you --
23 MR. NIEBERG: Okay. And I'll just add we had a third response
24 in our sur-reply under their constructions. And if you look to the Axonics
25 case that we cited in our papers, that's on Slide 125, in our view this was a

1 new claim construction and that we had a good faith basis not to address
2 every possible claim construction. And so in response to their new
3 construction, we explained also, Foster anticipates and is obvious under that
4 construction.
5 I won't eat up any more time unless there's questions that you'd like
6 me to address.
7 JUDGE GIANNETTI: I think we're all set there. Thank you,
8 Counsel.
9 MR. NIEBERG: Thank you.
10 JUDGE GIANNETTI: And now we'll hear from the Patent Owner
11 for surrebuttal. Again, I'll remind you that your surrebuttal is limited to the
12 points raised by Counsel in rebuttal.
13 MR. LOWENSTEIN: Thank you, Judge Giannetti. Since we
14 have, I believe, 31 minutes remaining and since we have to coordinate
15 amongst three different attorneys, may I request just a five-minute -- and you
16 can count against our time if you'd like. I don't think we're going to use 31
17 minutes. But we'd just like to talk amongst ourselves, get our ducks in a
18 row, and then we'll be back in five minutes. And if you want to --
19 JUDGE GIANNETTI: Okay. I'll ask -- we'll take a five-minute
20 in-place recess. I want everyone to stay online. You can turn your cameras
21 off if you like. But I want to make sure that we try to get this thing done on
22 time. So yeah, we're in recess for five minutes, but don't wander off. Thank
23 you.
24 (Whereupon, the above-entitled matter went off the record at
25 5:16 p.m. and resumed at 5:22 p.m.)

1 MR. LOWENSTEIN: Okay. Thank you, Your --
2 JUDGE GIANNETTI: All right. So let's proceed and let's have
3 your surrebuttal. I think you have, what is it, 31 minutes, Counsel?
4 MR. LOWENSTEIN: Correct. It's 26 minutes if you deduct the
5 five. I don't think we're going to use 26 minutes either.
6 JUDGE GIANNETTI: Okay, 26? All right. Fine. Just proceed,
7 and we'll see where we go with the time. But I think you'll probably have
8 enough time.
9 MR. LOWENSTEIN: So based on the issues that I argued, I didn't
10 hear any rebuttal on analogous art or the Foster-Hayhurst combination or the
11 issue with the chunks and packets. So I will not be addressing that at all
12 because there's nothing to respond to, unless there are any questions from
13 Your Honors.
14 The only issue that I argued that was addressed was I heard Mr.
15 Nieberg say that a good faith argument was presented, that the -- there's a
16 processor that's executing code to store. But a good faith argument is not the
17 quite the same thing as a good persuasive argument. And I still have not
18 heard any urgent explanation for how it is that the processor in Foster's
19 system is executing code to effective storage on this external set-top box.
20 I did not hear any response to that. I heard some argument
21 presented on obviousness, but I did not hear a response to the arguments that
22 I made. As I said, Foster has no need for this change. It would make Foster
23 less secure. And so a POSITA would not be motivated to do it. And I didn't
24 hear any response to that.
25 With that, I will turn things over to Ms. Sanders and then Mr.

1 Iancu, unless there are questions.
2 JUDGE GIANNETTI: No.
3 MR. LOWENSTEIN: Thank you, Your Honors.
4 MS. SANDERS: Hello, again. My name is Haley Sanders, just
5 for the record. I first wanted to address Petitioner's arguments regarding -- I
6 believe it was their -- our Slide 190, talking about the nearly perfect security
7 of Tajima. And while Petitioner is correct that this -- Dr. Bhattacharjee was
8 not talking directly about Tajima, he was talking about a system that is
9 designed exactly like Tajima.
10 And that particular analogy, you have data put on a USB drive and
11 data kept on a computer. And just like in Tajima, you take that smaller
12 portions of a data set, and you separate it. You have the data on a USB drive
13 and on the computer, and those are two separate areas under separate
14 control.
15 So if someone were to hack into your computer, he's not also in
16 your pocket with the USB drive. And if someone were to pickpocket you,
17 he doesn't have access to your computer. So this is nearly perfect security
18 because it is storing data and key information in separate areas under
19 separate control. It's that separate control that's really key to the security
20 here.
21 And I also wanted to speak on Petitioner keeps repeating that this
22 key encryption key scheme is so well-known in the prior art, it's so common,
23 and would have been implemented so easily by a POSITA. So if that was
24 the case, the inventors in Tajima would have known that. But they chose not
25 to implement a key encryption key scheme. That was a choice. The

1 inventors in Tajima thought that their security was enough to address the
2 issue.
3 And further, the implementation of a key encryption key
4 management system was something that Petitioner explicitly said was
5 against the goal of Tajima. In their petition at page 22 and reply at 8, they
6 said that Tajima discloses for, i.e., "a system that needs only the key
7 information to decrypt data fragments and not additional key management
8 infrastructure."
9 And my next point, I wanted to say that Petitioner says that
10 Foster's key encryption key provides security because it requires an attacker
11 to break into a separate system with separate security in order to access the
12 KEKs, to decrypt the key information, and access the data chunks. But that
13 separate control, again, and separate security is exactly what Tajima
14 implements, so that, again, Tajima has no need for Foster's key encryption
15 key.
16 And did I --
17 MR. LOWENSTEIN: Just explain that to them, but that you have
18 to go to a separate slide --
19 MS. SANDERS: So again, Petitioner posits that Foster provides
20 security because in order to access the KEKs to decrypt the key information,
21 you have to break into a system under separate control with separate security
22 outside of Tajima's system. And that's already the case in Tajima, as I've
23 explained.
24 So you store data fragments with key information that cannot
25 decrypt the data fragments. And you split them into separate areas under

1 separate control with different firewalls, different access privileges, different
2 using privileges. And in that way, the data siloed from one another and
3 again provides that that is why it provides that nearly perfect security.
4 Okay. And unless there's any questions, that's all I have.
5 JUDGE GIANNETTI: All right. Thank you very much, Counsel.
6 Any further surrebuttal here?
7 MS. SANDERS: I will pass it over to Mr. Iancu.
8 JUDGE GIANNETTI: Okay.
9 MR. IANCU: All right. Your Honors, just a couple more points to
10 address what Petitioner Counsel said in rebuttal. I have to say I very much
11 enjoy the various analogies with the keys and alarm bells and umbrellas in
12 particular. And I don't want to go back to the analogies. Instead, I just want
13 to make it -- make the point clear that those of skill in the art understand that
14 you just can't add layer upon layer with no consequence.
15 And if we look at SFI Slide 160, which we have on the screen right
16 now, I commend Your Honors to Exhibits 2007, page 4, and Exhibit 2008,
17 page 2. These are treatises from reputable experts in the field -- will make it
18 clear, as it said in Exhibit 2008, that it is possible to build a weak
19 cryptographic system using strong algorithms and protocols.
20 And if we go to the Slide 161, I already showed this the first time
21 around that it's really hard to do key management systems. In fact, it might
22 be the hardest part of cryptography. You can't just wave your hands and say,
23 oh, it was known. You need to be specific about it. And Petitioner was not
24 very specific about it at all in the petition.
25 To be clear, these new arguments that we're hearing now about

1 external management of key encryption keys, KEKs, is basically new to
2 their rebuttal. If we go to Slide 162, in their petition, what we know is
3 that -- or what they argued is that the Orsini reference, for example, does
4 external session key management.
5 Okay. The Orsini reference talks about the session key. And
6 remember, the master session key in Figure 21 is -- I think at the very
7 beginning of the figure -- where you have the master session key for that
8 particular session that you use to encrypt the data in the first place in the
9 very different encryption scheme in that particular embodiment. That's the
10 session key there. And the management of that session key is described in
11 our CDM.
12 That is the only thing petition -- the petition pointed to. And they
13 described in the petition, you know, how to do that. And, you know, they
14 cite various paragraphs of Orsini about how to manage the session master
15 key. But then we presented lots of evidence from our expert, Dr. Rubin,
16 about that in our Patent Owner response and the Rubin declaration.
17 And for example, if we go to the next slide, Slide 163, we
18 explained how it's very different to manage session keys from key
19 encryption keys, which is where they now are from their reply. And it's
20 different because while the session key needs to be changed often, perhaps
21 daily, the key encryption key doesn't have to replace as frequently, maybe
22 once a year. That's one explanation.
23 If we go to Slide 164 --
24 JUDGE GIANNETTI: Counsel, doesn't that make them
25 advantageous? Wouldn't the person of ordinary skill -- aren't you making an

1 argument that a person of ordinary skill in the art would use key --
2 encryption keys, because they're advantageous?
3 MR. IANCU: In some embodiments, if you have a different
4 encryption scheme altogether, perhaps. But not in the Orsini embodiment,
5 for sure. Because as we discussed in the first go-round, in the Orsini
6 embodiment, it's a complete encryption -- a security mechanism there with
7 two layers of encryption of the data itself, a layer of encryption of the
8 session key, and then, importantly, an obfuscation scheme.
9 And for the reasons I've discussed the length of the -- when I was
10 up here the first time, it makes no sense to add yet another key encryption
11 key layer on top of all of that.
12 JUDGE GIANNETTI: Okay. I thought you were making a case
13 for using key encryption keys.
14 MR. IANCU: No, no, no. So all I am saying here is that Petitioner
15 did not rely on the key encryption key scheme or argument in the petition.
16 JUDGE GIANNETTI: It was a rebuttal to your argument, though,
17 wasn't it?
18 MR. IANCU: Yeah. It was a rebuttal to the argument. They
19 added this additional argument. And what I'm answering here is the
20 question posed, where is the explanation of how to manage this -- the new
21 key encryption key argument that they provided. If you're going to add the
22 key encryption key, as they say in rebuttal, how are you managing it? That's
23 the question posed.
24 JUDGE GIANNETTI: Well, I think their point -- the point that
25 they made is that that's well-known.

1 MR. IANCU: Well, that's the point --
2 JUDGE GIANNETTI: Not only is the use of key encryption key is
3 well-known, and I don't think you deny that, but also their management is
4 well-known. I think that's their argument.
5 MR. IANCU: That is their argument. But what I'm saying is --
6 JUDGE GIANNETTI: It's a detail that doesn't need to be
7 disclosed to a person of ordinary skill in the art because they would know
8 how to do it.
9 MR. IANCU: Right, that's their argument. And I'm responding to
10 that argument by saying that's wrong.
11 JUDGE GIANNETTI: Okay.
12 MR. IANCU: It's one thing to say, yeah, it's generally known how
13 to manage the security of a key encryption key, but it's a completely
14 different thing to explain with particularity how you would do it with respect
15 to the Orsini reference after that whole scheme is already disclosed.
16 Where and how are you managing -- when you have, perhaps, you
17 know, millions of shares you have to deal with and now you're adding yet --
18 that's obfuscated and encrypted -- now you're adding another encryption
19 there, where are you putting that key and how are you managing that?
20 JUDGE GIANNETTI: So your argument, Counsel, is that this
21 would be beyond the skill level of the person of ordinary skill in the art, is
22 that -- that's your argument.
23 MR. IANCU: Exactly. That it was not disclosed in Orsini. It's not
24 common knowledge at all. And it is -- most importantly, to answer a
25 question posed by His Honor, which is where in the record did you describe

1 that, Petitioner? And what I'm saying is they didn't. They did not describe
2 that in the petition.
3 Okay. And --
4 JUDGE GIANNETTI: But that's their rebuttal argument. You're
5 arguing that it's not a fair rebuttal?
6 MR. IANCU: No, no, no. I'm just saying that they didn't describe
7 how to -- they only pointed to the session key. And then in their rebuttal
8 argument, to end on this point, let me go to Slide 166, here is the rebuttal
9 argument about how to do this complicated issue.
10 Okay. So they're saying Orsini already taught techniques for
11 managing and securing other KEKs or at least could have been modified in a
12 simple straightforward way, to use conventional techniques for doing so.
13 And what's their evidence for this?
14 As discussed below, Orsini supports prior art triple DES and AES.
15 And they cite paragraph 378. This is their evidence about how to manage
16 KEKs in rebuttal, paragraph 378 of Orsini, which says nothing about KEKs,
17 that it says that Orsini could also be used in a scheme with triple DES and
18 AES and that you got to go to those things. And those things will somehow
19 tell you how to manage KEKs.
20 But even if they do -- it's not here. But even if they do, they're not
21 going to tell you how to manage them with respect to a system, a security
22 system that already has complete security, including -- as described by -- as I
23 described at the beginning, including multiple encryption levels and an
24 obfuscation level.
25 And just to leave with this final thought, the Orsini reference

1 teaches a particular encryption scheme, as I've mentioned. It does not teach
2 the scheme of the patents before Your Honors. Their argument is -- they're
3 asking -- but they're saying it's obvious, even though it's many of the same
4 inventors et cetera who didn't think about it in the first go-round.
5 How do we know it's obvious? Well, because it was done in the
6 patents -- in the later patents. This is the most prototypical hindsight use of
7 the patents before us to supply the missing limitations or the missing
8 combinations. And it just cannot be that the explanation for why a prior art
9 reference does not teach the later reference -- or is -- I'm sorry, it makes the
10 later reference obvious.
11 It cannot be the answer that, well, the later reference did it. That
12 would be completely circular and it would eat up the entirety of patent law.
13 But that's not what, you know -- and here, I think as we have seen top to
14 bottom, the patents before the Board, all three of them provide the brand
15 new -- or multiple, different brand-new encryption schemes. And this is a
16 complex area of art. Nobody else before these inventors came up with these
17 schemes.
18 And for that reason, Your Honors, we urge the Board to affirm the
19 validity of all three patents. Thank you.
20 JUDGE GIANNETTI: All right. Thank you, Counsel. Any
21 further questions from the panel?
22 JUDGE BELISLE: None for me.
23 JUDGE GIANNETTI: Hearing none. I will say that we appreciate
24 the effort that was put into preparing this argument and we appreciate your
25 argument. And we will take the case under advisement. And we, especially,

1 would like to thank our LEAP practitioner, congratulate her on her first
2 argument which went very well, and also thank her colleagues and her client
3 for allowing her to participate in this program.
4 And with that, the case is under submission. And we are
5 adjourned. We will ask the parties to stay on the line with the court reporter
6 and make sure that there aren't any questions, spellings, et cetera. Again,
7 thank you and good evening, everyone.
8 (Whereupon, the above-entitled matter went off the record at 5:40
9 p.m.)

PETITIONER:

Elisabeth Hunt
Greg Nieberg
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
gnieberg-ptab@wolfgreenfield.com

PATENT OWNER:

Stephen Elliott
Andrei Iancu
SULLIVAN & CROMWELL LLP
elliotts@sullcrom.com
iancua@sullcrom.com

Kenneth Weatherwax
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com