

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA and KAHOOT EDU, INC.,
Petitioner,

v.

AVIEL D. RUBIN,
Patent Owner.

IPR2023-00693
Patent 9,064,376 B1

Record of Oral Hearing
Held: July 12, 2024

Before KEN B. BARRETT, KEVIN W. CHERRY, and
CYNTHIA L. MURPHY, *Administrative Patent Judges*.

IPR2023-00693
Patent 9,064,376 B1

APPEARANCES:

ON BEHALF OF THE PETITIONER:

BRIAN BANNER, ESQUIRE
Slayden Grubert Beard PLLC
401 Congress Avenue, Suite 1650
Austin, Texas 78701 U.S.A.
512-402-3550

RUDOLPH KIM, ESQUIRE
Paul Hastings LLP
1117 S. California Avenue
Palo Alto, California 94304
650-320-1830

ON BEHALF OF THE PATENT OWNER:

ROBERT McARTHUR, ESQUIRE
ERIC BENISEK, ESQUIRE
Vasquez, Benisek & Lindgren, LLP
1550 Parkside Drive, Suite 130
Walnut Creek, California 94596
925-637-4250

ALSO PRESENT, OBSERVING: DR. AVIEL RUBIN, PATENT OWNER

The above-entitled matter came on for hearing on Friday,
July 12, 2024, commencing at 1:00 p.m., via video-conference.

P R O C E E D I N G S

- - - - -

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

JUDGE BARRETT: Thank you. Okay, then. We are on the record in IPR2023-00693, *Kahoot! v. Rubin*. This is a virtual hearing today being conducted by video conferencing. I am Judge Barrett, and with me today are Judges Cherry and Murphy.

Let's get started today with the parties' appearances. Who do we have for Petitioner?

MR. BANNER: Good afternoon, Your Honors. My name is Brian Banner with Slayden Grubert Beard on behalf of Petitioners Kahoot. And also with me today is Rudy Kim, co-counsel at Paul Hastings, on behalf of Petitioners.

JUDGE BARRETT: Thank you and welcome. And who do we have for Patent Owner today?

MR. McARTHUR: Good afternoon, Your Honors. Rob McArthur, Vasquez, Benisek, & Lindgren. With me is co-counsel Eric Benisek. And Patent Owner Dr. Aviel Rubin is also attending. Mr. Benisek will be presenting the argument today.

JUDGE BARRETT: All right. Thank you and welcome.

MR. McARTHUR: Thank you.

JUDGE BARRETT: We set forth the procedure for the hearing today in our oral argument order. But just as a reminder, Petitioner will have 60 minutes total to present its arguments, and Patent Owner also will have 60 minutes total. Petitioner will go first and may reserve time for rebuttal. Patent Owner then will have the opportunity to present its response and may reserve -- I'm sorry. Petitioner will go first, then Patent Owner. Patent

1 Owner may reserve some time for a surrebuttal. Petitioner then will present
2 its rebuttal. Patent Owner will then present its surrebuttal arguments.

3 Is that procedure acceptable to everyone? Petitioner?

4 MR. BANNER: Yes, Your Honor. This is Brian Banner. That's
5 acceptable.

6 JUDGE BARRETT: Patent Owner?

7 MR. McARTHUR: Yes. Yes, Your Honor.

8 JUDGE BARRETT: All right. Thank you.

9 MR. McARTHUR: That's acceptable to the Patent Owner.

10 JUDGE BARRETT: Great. All right. We do have your
11 demonstrative exhibits pulled up on our computers, and we have access to
12 the record. You are free to present if you want to share your screen. Some
13 people do that, some people don't. Conduct your hearing as you see fit. It
14 all works for us. Regardless, for clarity of the transcript and to assist the
15 Judges in following along, if you would, please, anytime you refer to a
16 demonstrative exhibit, please state the slide number. Or if you're going to
17 pull something from the record, give us exhibit number, column, line, page,
18 whatever is appropriate, so we have a good, clean record to look back on.

19 These hearings are open to the public, and there is, in fact, an open
20 public line. I don't expect any confidential information to come out today,
21 but if you sense that there might be some coming up, just pause, let me
22 know, and we'll deal with it as is appropriate.

23 And I think that's all I've got. Any questions or concerns, Petitioner?

24 MR. BANNER: None on behalf of Petitioner.

25 JUDGE BARRETT: Okay. Patent Owner?

26 MR. McARTHUR: None on behalf of the Patent Owner.

1 JUDGE BARRETT: All right, then. With that, Petitioner, you may
2 begin whenever you are ready. And if you could start by telling me how
3 much time you'd like to reserve.

4 MR. BANNER: Thank you, Your Honor. I would like to reserve 15
5 minutes of the time for rebuttal. And I plan to share the presentation through
6 screen sharing while I go through it. So, if that's all right, I will start sharing
7 my screen now.

8 And I believe I'm sharing my screen.

9 JUDGE BARRETT: We can see, there we go, we can see your slides.

10 MR. BANNER: Okay, perfect. So starting at slide 1, and I will begin
11 now. May it please the Board. My name is Brian Banner, and I'm here on
12 behalf of Petitioners Kahoot! ASA and Kahoot Edu. I want to thank the
13 Board for the opportunity today to present on behalf of Petitioners and
14 explain why we believe that the Board should find the revised substitute
15 claims to be unpatentable. We've submitted demonstratives, and as I just
16 mentioned, I will be moving through those demonstratives during my
17 presentation.

18 Moving to slide 2 of the demonstratives. For the Board's reference,
19 slide 2 contains a table summarizing the asserted grounds of invalidity.
20 Typically, these are found in the petition, but due to the motion to amend
21 practice, we've included this summary here. It's also found in the text of
22 Petitioner's opposition to the revised motion to amend, and that's scattered
23 throughout the grounds in paper 27.

24 Slide 3. So here's the agenda that I plan to go through today. I plan
25 to use about 45 minutes of my time and would like to reserve the remaining
26 time for rebuttal. I'll start with an overview of the revised substitute claims.

1 Then I'll cover the 112 deficiencies, then claim construction. Then I'll
2 discuss the grounds based on the prior art *Zha* reference, followed by the
3 grounds based on the *Kling* and *Lim* references. If I have time remaining, I'll
4 finish with the grounds based on the *Takahashi* reference.

5 JUDGE MURPHY: Mr. Banner, can I interrupt you just for a second?
6 Could you go back to the grounds slide, please?

7 MR. BANNER: Certainly.

8 JUDGE MURPHY: Okay. If I understand correctly, you're not
9 challenging claim 36, correct?

10 MR. BANNER: No, we are not challenging claim 36. That's correct.

11 JUDGE MURPHY: Okay. Thank you.

12 MR. BANNER: Slide 4, revised substitute claims. So, as the Board
13 may recall, the Patent Owner's motion to amend is non-contingent. Thus,
14 Patent Owner is not disputing that the prior art discloses or teaches the
15 limitations in the original claims. Instead, Patent Owner has added these
16 additional limitations to claims and presents arguments based on the new
17 limitations.

18 Slide 5. What are the new limitations? So in this slide we show in
19 claims 26[c] and 41[d] there are new limitations related to using "application
20 specific authentication information that is not authentication information
21 specific to a device at both the first and second devices." This limitation
22 requires that the authentication information be application specific. It also
23 has to be device independent, so not specific to a device.

24 The other limitation in claim 26[c] and 41[d] that has been added is
25 "wherein the application specific authentication information used on the first
26 device is different from the application specific authentication information

1 used on the second device." So here different authentication information is
2 used by the two different devices. Claim 28 has a new limitation that the
3 sensitive information is only shared with the second device.

4 Slide 6. Patent Owner has also added what Petitioner believes to be
5 non-limiting language to the claims. There is a phrase "protecting
6 information by," which is added to the preamble of claims 26 and 41. And
7 Patent Owner also added a thereby clause to claim limitations 26[d] and
8 41[e], which I will discuss when I get to claim construction. Patent Owner
9 made additional changes to claims 30 and 35, but we don't believe those are
10 in dispute as the prior teaching related to those claims are not disputed and
11 so I won't be covering those today.

12 Slide 7. So starting off with the 112 deficiencies.

13 Slide 8, summary of those deficiencies. This slide contains a
14 summary of the three 112 issues. The first is a lack of written description
15 support for claims 26 and 41 related to the claim phrase "application specific
16 authentication information that is not authentication information specific to a
17 device at both the first and second devices." The second 112 issue relates to
18 claim 28 and a lack of written description support for the new limitation,
19 "the sensitive information is only shared with the second device." And the
20 third 112 issue relates to claims 32 and 35, where the phrase "the
21 information displayed on the respective devices" is indefinite.

22 Slide 9. So I'm going to start with the written description challenge
23 for claims 26 and 41.

24 Slide 10. This shows the claim language for substitute to claim
25 limitation 26[c]. At issue is the phrase "not authentication information
26 specific to a device at both the first and second devices."

1 Slide 11. Now, this is a negative limitation. That is, it is not device
2 specific at both the first and second devices, and Patent Owner argues in its
3 reply at page 2 that the written description sufficiently describes this
4 negative limitation by excluding non-device specific authentication
5 information and disclosing this precise embodiment. However, the '995
6 application discusses the negative limitation only in the context of the
7 second device. That is, excluding non-device specific authentication
8 information is discussed only with respect to the second device.

9 Now, we see this in paragraph 92 of Exhibit 2005, which is the only
10 portion of the specification that discusses a device independent password.
11 Paragraph 92 is limited to a discussion of the second device. It does not talk
12 about the first device.

13 Patent Owner cites to the Federal Circuit's *Novartis* case at pages 1
14 and 2 of its reply. *Novartis* provides the test for determining whether a
15 negative limitation has written description support and requires that the app
16 specification describe a reason to exclude the relevant element. Here, where
17 the specification is talking only about device independence for the second
18 device, the specification does not meet that legal test. It does not describe a
19 reason to exclude device specific authentication for the first device, and
20 that's why we believe that this limitation is not supported by the written
21 description.

22 Slide 12. Finally, Patent Owner in its reply assumes that the
23 discussion in paragraph 92 would just apply to the first device. However,
24 nothing in the specifications states that passwords are always device
25 independent, and, in fact, Patent Owner argues that the prior art *Kling's*
26 password for the second device is not device independent. So Patent Owner

1 can't have it both ways when it's talking about the written description
2 requirement, and then have it another way when it's talking about trying to
3 distinguish prior art. The written description does not satisfy what is needed
4 for a negative limitation and, therefore, claims 26 and 41 should not be
5 allowed. And I will note that this issue is dispositive as it affects all of the
6 revised substitute claims.

7 Slide 13. Moving to the next 112 issue claim 28.

8 JUDGE MURPHY: Counselor, can I stop you for a second? Can we
9 go back to paragraph 92, back to the slide with paragraph 92? Isn't this
10 paragraph saying, though, that if you have a password that -- on an
11 electronic device that it doesn't have to be -- it cannot be -- it doesn't have to
12 be device specific? In other words, isn't it sort of saying that when the
13 previous paragraphs described the first device as having the password and
14 the second device as having a password, but no authentication token, doesn't
15 the specification convey that in those instances the passwords for both of the
16 devices are not device specific? Excuse me.

17 MR. BANNER: I think that that's what Patent Owner's argument is.
18 But I think when you actually look at what 92 says is 92, paragraph 92, is
19 only talking about the second device. So yes, the previous paragraphs
20 disclose that passwords are used for both the first and second devices. But
21 what Patent Owner is trying to do is add a negative limitation that says the
22 password used on the first device excludes or must be device independent.
23 And nowhere in any of the previous paragraphs is that disclosure made.
24 And that's the problem with the addition here, is that it's a negative
25 limitation. There's no dispute about that. Patent Owner agrees it's a
26 negative limitation. And so in order to meet the *Novartis* test, there has to be

1 some reason to exclude device specific authentication on the first device.
2 That's simply not stated anywhere in the app specification. And that's why
3 we believe that this limitation, the new limitation, is not supported under the
4 *Novartis* test for negative limitations.

5 JUDGE MURPHY: But you're agreeing that this paragraph 92
6 supplies support for the second device having authentication that is not
7 device specific, correct?

8 MR. BANNER: Yes, we agree with that. And so if that's the
9 limitation they wanted to add, we would not take issue with that.

10 JUDGE MURPHY: Thank you.

11 MR. BANNER: All right. Moving back to slide 14. So claim 28
12 lacks written description support for the phrase sensitive information is only
13 shared with the second device.

14 Here's the claim language, moving to slide 15. The reason this
15 phrase lacks written description support is because every embodiment
16 contemplates sharing sensitive information beyond the second device. In
17 fact, Patent Owner admits that the sensitive hole cards in the poker
18 embodiment are shared with the first device. Patent Owner argues that the
19 information is no longer sensitive when they are shared. But the claim
20 language does not contemplate sharing at a later time or that the information
21 can become non-sensitive. And the patent does not say that the hole cards
22 are no longer sensitive.

23 Rather, at column 5, lines 56 to 63 of Exhibit 1001, the patent says
24 the hole cards are sent to the first device so that a record of the hand
25 histories can be kept. Patent says that the cards have diminished value, not
26 that they are no longer sensitive. So because all of the embodiments share

1 sensitive information beyond the second device, we don't believe there's any
2 written description support for this new limitation, which says hole cards can
3 only be shared with the second device.

4 Slide 16, the indefiniteness challenge on claims 32 and 35.

5 Slide 17. The scope of the phrase "the information displayed on the
6 respective devices" in claims 32 and 35 cannot be determined with
7 reasonable certainty. And here's the claim language, claims 32 and 35. And
8 this has to do with the graphical identifiers indicating a link between the
9 information displayed on the respective devices.

10 Slide 18. So Patent Owner does not dispute that this phrase lacks
11 antecedent basis. Instead, in trying to describe the scope of this term, Patent
12 Owner offers four different explanations of varying scope. Patent Owner's
13 expert offers even a different explanation, and these are all found in Patent
14 Owner's reply. That's Paper 30 at pages 3 and 4. And the fact that even
15 Patent Owner can't concisely define the scope of this term confirms that it is
16 indefinite, as its scope cannot be determined with reasonable certainty.

17 I'd like to move to claim construction now, slide 19 and then slide
18 20. So there are two new phrases in the revised substitute claims that we
19 believe require construction. First, there's a preamble phrase, "for protecting
20 information," that's been added to claims 26 and 41. And limitations 26[d]
21 and 41[e] include a thereby clause, which is, "thereby protecting the second
22 subset of information from potential malware on the first device." Patent
23 Owner argues that these phrases limit the claims, but these phrases are non-
24 limiting because they recite nothing more than a result of performing the
25 other claim steps.

1 Slide 21. And the legal test for this is from *Texas Instruments* case.
2 That's the Federal Circuit in 1993. And according to the Federal Circuit in
3 this case, "A whereby clause that merely states the result of the limitations in
4 the claim adds nothing to the patentability or substance of the claim." And
5 that's exactly what we have here with the Patent Owner's thereby clause.

6 Slide 22. So here's the claim language. Claim 26[d] limitation is
7 reproduced here. Claim 41[e] has the same limitation. In both claims we
8 have a positive recitation prior to the thereby clause of, "transmitting the
9 second subset of information to the second device from the server, wherein
10 the second subset of the information includes information not transmitted to
11 the first device."

12 Now, Patent Owner's expert Dr. Traynor confirms that this
13 transmitting limitation protects the second subset of information from
14 malware. So at the bottom of this slide is a quote from paragraph 84,
15 Exhibit 2009, in which Dr. Traynor states, "The claims require that a second
16 subset of information is sent by the application to only the second device."
17 So he's referring to the transmitting limitation I just quoted, and that's
18 underlined above from claims 26[d] and 41[e].

19 Dr. Traynor goes on to explain that, "This isolation of information
20 provides protection to the second subset of information because it is not
21 exposed to malware that has potentially compromised the first device." So
22 protection is provided by the positive limitation of transmitting the subset of
23 information only to the second device. Dr. Traynor admits this fact.
24 Because of that the thereby clause, which says protecting the second subset
25 of information not transmitted to the first device from potential malware on

1 the first device, merely states the result of the previous limitation. Under the
2 *Texas Instruments* case, the thereby clause is therefore non-limiting.

3 Slide 23. Moving into the *Zha* grounds.

4 Slide 24. As the Board may recall, *Zha* is a reference that discloses a
5 microblog application, like a social media platform, that a user can log into
6 and access simultaneously with two different terminals. On the left side of
7 slide 24, we have a quote from *Zha*, Exhibit 1004 at column 4, lines 21
8 through 24, as well as figure 1, which shows the system with terminal 1 as a
9 cellphone, terminal 2 as a laptop, and another terminal as a desktop
10 computer. These terminals can all access the server 120, which is running
11 *Zha*'s microblog application. On the right of slide 24 is a quote from column
12 18, lines 11 through 17 of Exhibit 1004, which states that the user can log
13 into the microblog with the cellphone, the laptop computer, and the desktop
14 computer simultaneously and send simultaneous application requests for the
15 three terminals.

16 Slide 25. As the Board may recall from the Institution Decision, and
17 again from the preliminary guidance that was provided, *Zha* discloses all of
18 the original claim limitations. The Board found a reasonable likelihood that
19 Petitioner would prevail, and proving that original claim 1 would have been
20 obvious over *Zha*.

21 Slide 26. At page 18 of the Institution, the Board found that *Zha*
22 discloses a login process to determine whether a single user has logged into
23 the same microblog application at two different terminals. This is not
24 disputed.

25 Slide 27. At page 19 of the Institution Decision, the Board also
26 found that *Zha* discloses the first and second subsets of information are

1 transmitted if and only if a user is logged into the microblog application with
2 two devices. That finding is also undisputed.

3 Slide 28. So what are the disputes?

4 Slide 29. Patent Owner makes essentially four arguments, and I'll
5 briefly summarize those four arguments, and then following a brief
6 summary, we'll walk through the evidence for each of them that shows why
7 Patent Owner's arguments are wrong.

8 The first argument Patent Owner makes is that *Zha* fails to disclose
9 authenticating a user on two devices as claimed in 26[c], which requires
10 using different application specific authentication information that is not
11 device specific. The Board's preliminary guidance at page 19 correctly
12 concludes that *Zha* plus a POSITA's knowledge teaches authentication or
13 login from two devices using passwords as the application specific
14 authentication information. In addition, using different passwords for
15 different devices would be obvious based on the teaching of *Gui*. So
16 whether we rely on a POSITA's knowledge or an express combination of
17 *Zha* and *Gui*, claim 26[c] is obvious.

18 Slide 30. The second argument Patent Owner makes is that *Zha* fails
19 to disclose protecting information as recited in the thereby clause of claim
20 26[d]. As already discussed, these limitations are non-limiting. But even if
21 they are limiting, *Zha* discloses protecting private information -- private
22 messages from malware by sending private messages only to the cellphone.

23 Slide 31.

24 JUDGE MURPHY: Counselor, can I stop you for a second and go
25 back to the previous slide?

26 MR. BANNER: Certainly.

1 JUDGE MURPHY: Does *Zha* talk about the security of the private
2 message from the standpoint of malware or the security of that? Because I
3 recall that *Zha* really talks about not having to switch interfaces on the first
4 device. That's more the focus. The problem that they're looking at is
5 switching interfaces. So if you have two interfaces open at the same time,
6 you don't have to switch back and forth. Can you point me to something in
7 *Zha* that talks about this being also, in addition to this interface switching
8 convenience, this also being a security against computer malware and other
9 kind of security concerns?

10 MR. BANNER: No, I can't point to anything specifically in *Zha* that
11 relates to security or malware. What I can tell you is that the isolation of the
12 information, and I'll go through this in the evidence, but Dr. Traynor has
13 testified that when you isolate information to one device, when you send it
14 specifically to one device, you're automatically protecting that information.
15 We saw that before when I was talking about the claim construction. And so
16 while *Zha* may not say, hey, this provides better security or this protects
17 against malware, the default -- actually the result of what's happening here is
18 when the private messages are sent to the cellphone and only the cellphone,
19 those private messages are protected from discovery by malware on the first
20 device.

21 So *Zha* doesn't say malware, it doesn't say security, but the sort of de
22 facto result of what *Zha* is doing would result in more secure private
23 messages.

24 Moving to slide 31, the third argument Patent Owner makes is that
25 *Zha* fails to disclose the sensitive information is only shared with the second
26 device, as recited in claim 28. *Zha* expressly discloses an embodiment

1 where private messages are sent only to the cellphone. And really, that
2 should be the end of the inquiry.

3 Patent Owner's teaching away argument here and throughout its
4 reply with other grounds does not satisfy the legal test for teaching away,
5 and I'll discuss that more. But finally, Patent Owner's interpretation of the
6 limitation where sensitive information cannot be shared beyond the second
7 device would really exclude every embodiment in the '376 patent, as we
8 discussed previously.

9 Slide 32. The fourth argument Patent Owner makes is, and this is
10 the final one for *Zha*, is that *Zha* is not analogous art. And this may get back
11 to what Your Honor was asking about with requests of malware and
12 security. The Board dismissed this argument in its preliminary guidance,
13 and we believe that the Board's conclusion there is correct. The Patent
14 Owner relies on the point of novelty and the problem to be solved to define
15 the field of endeavor, which is contrary to law. But more importantly,
16 Patent Owner has attempted to add non-limiting phrases, so the protecting
17 information phrase in the preamble and the thereby clause, in order to
18 change the field of endeavor for this patent. But that should not affect the
19 field of endeavor as it would really encourage mischief by Patent Owners
20 faced with invalidating prior art in inter partes reviews if all I have to do is
21 come in as a Patent Owner and add some non-limiting language and say this
22 isn't the field of the art that was presented in this IPR. That seems like that
23 would be an easy out for Patent Owners.

24 So let's look at the evidence related to these arguments. On Slide 33
25 is Patent Owner's first argument that *Zha* does not teach different application
26 specific authentication information for different devices.

1 Slide 34. *Zha* does, in fact, disclose using application specific
2 authentication information. The Board found this in its preliminary
3 guidance, page 19, because "*Zha* disclosing a user logging into the account
4 of a microblog application program through two or more terminals appears
5 to correspond to providing information for authentication that is specific to
6 the microblog application." That does not appear to be disputed.

7 Slide 35. In fact, both experts agree that passwords were well known
8 authentication information used for accessing online applications. So while
9 *Zha* doesn't say you use a password to log in, this was a well-known thing at
10 the time.

11 At paragraph 196 of Exhibit 1029, Dr. Meldal states that it "was well
12 known by 2014 that password authentication could be used for logging into
13 an application such as *Zha*'s microblog." Dr. Traynor co-authored a 2006
14 article that notes that, "Passwords are currently the dominant authentication
15 mechanism in computing systems." That's Exhibit 1024 zero zero one.
16 Thus, when *Zha* discusses logging into the microblog, a POSITA would
17 understand that would likely be done with password authentication.

18 Slide 36. According to Patent Owner, passwords for accessing
19 online applications are application specific and not device specific. At page
20 2 of paper 30, that's Patent Owner's reply, the Patent Owner states that
21 limiting the authentication process to non-device specific authentication
22 information "was a known concept to a POSITA and applied to all devices
23 attempting to access web applications." So there appears to be no serious
24 dispute that device independent passwords were the predominant means to
25 access an online application, at least by the time the '376 patent was filed.

1 Slide 37. The only remaining aspect of the new claim 26[c]
2 limitation is that the different devices would use -- in *Zha* would use
3 different authentication information. And here's where we turn to the *Gui*
4 reference. That's Exhibit 1031.

5 *Gui* provides evidence that a POSITA would know to use different
6 passwords with different devices. *Gui* also provides express motivation for
7 using different passwords with different devices. At Exhibit 1031, column
8 2, lines 20 through 29, *Gui* explains that the present invention "provides
9 system and methods for the association of multiple sets of credentials to a
10 single user account. This enables the user to easily access computer based
11 services using devices that have different form factors, data input
12 techniques, and security capabilities.'

13 Slide 38. *Gui* discusses why a POSITA would use different
14 passwords on different devices to access online applications. At Exhibit
15 1031, column 1, line 39, through column 2, line 3, *Gui* addresses a problem
16 that arises when different devices are used to access a computer based
17 service. Different devices have different form factors as well as different
18 data input capabilities. Because of this, a POSITA would know to use
19 different passwords for the different devices.

20 *Gui* gives the examples of trying to enter special characters on a
21 cellphone before the days of smartphones, and some of us have similar
22 problems today trying to enter passwords using a remote control to peck at
23 the keyboard interface on modern TVs. It can be cumbersome based on
24 what your input device is.

25 So slide 39. At paragraph 241 of Exhibit 1029, Dr. Meldal
26 summarizes the motivation *Gui* provides to use different passwords with

1 different devices. He states, "At the time of the '376 patent, *Gui* teaches that
2 some passwords are more difficult to enter on a mobile phone compared to
3 entering the same password on a computer that has a full keyboard. *Gui*
4 suggests an easy solution to this problem for any service that allows login to
5 the same account by both mobile phones and desktop and laptop computers.
6 *Gui*'s solution is to allow the user to have multiple passwords for logging
7 into the same account or service."

8 There are two other references, *Lipetz* and *Kling*. I discuss *Kling*
9 later. Those references also provide evidence of a POSITA's knowledge that
10 different passwords can be used for accessing the same application, and Dr.
11 Meldal discusses those references at paragraphs 200 to 204 of his
12 declaration, Exhibit 1029.

13 JUDGE MURPHY: Counselor, can you go back just one second for
14 me?

15 MR. BANNER: Certainly.

16 JUDGE MURPHY: Do these references teach that you're using
17 different passwords when you're simultaneously in the same application with
18 two devices? Or do they just say, if I use my phone for an application, I'll
19 use this, and then if tomorrow I want to use my computer, you know, my
20 laptop computer, I would have a different password for that?

21 MR. BANNER: *Gui* is silent as to whether or not it's simultaneously,
22 but I do believe that *Kling*, which we will talk about in a minute here, is with
23 simultaneous access with both a desktop PC and a mobile phone.

24 JUDGE MURPHY: Thank you.

25 MR. BANNER: You're welcome.

1 Slide 40. The *Zha* grounds 1 through 8 rely on the POSITA's
2 knowledge that different passwords can be used with *Zha*'s microblog, and
3 *Gui* and *Kling* are evidence of that knowledge. Alternatively, for grounds 9
4 through 16, *Gui* can be expressly combined with *Zha* to provide different
5 passwords with *Zha*'s different devices.

6 Slide 40 [sic]. At Exhibit 1029, paragraphs 209 to 210, Dr. Meldal
7 explains that *Gui* provides an express motivation to modify *Zha*'s microblog
8 application. As Dr. Meldal explains, "*Gui* provides additional motivation to
9 use multiple passwords in a system such as *Zha* that utilizes different
10 hardware devices," and that's human interface accessibility. As evidenced
11 by *Gui*'s disclosure, a POSITA's knowledge includes the understanding of
12 "the benefit of allowing multiple different passwords in a system like *Zha*
13 that provides for easy human interface access via desktop computer and
14 mobile phone. Accordingly, claim limitations 26[c] and 41[d] are rendered
15 obvious based on *Zha* and the POSITA's knowledge, or *Zha* combined with
16 *Gui*, where *Gui* discloses using different passwords on different devices.

17 And to go back to Your Honor's question about the simultaneous
18 access, we know that *Zha* specifically discusses and discloses accessing the
19 microblogs simultaneously from different devices. So to the extent there's a
20 question about the different passwords Petitioners rely on *Gui* as teaching
21 that while *Zha* allows for simultaneous access, that access can be using
22 different passwords at the same time.

23 So Slide 42. Moving to Patent Owner's second argument that *Zha*
24 fails to disclose protecting information as required by the preamble and the
25 thereby clause.

1 Slide 43. First, I have to mention that Patent Owner's argument
2 should be rejected because the preamble and thereby clause are not limiting.
3 But even if they are limiting, *Zha* discloses protecting the private message
4 information because private messages are sent only through the cellphone.
5 *Zha* discloses this at Exhibit 1004, column 19, lines 3 through 13. It says,
6 "The server may send a private message only to the cellphone without
7 sending the private message to the laptop computer or the desktop
8 computer."

9 As Dr. Traynor admits, and we've seen this already, this isolation of
10 the private message information, sending it only to the cellphone, protects
11 against malware on the other devices, such as a laptop computer or desktop
12 computer. That admission is at Exhibit 2009, paragraph 84.

13 Slide 44. Moving to Patent Owner's third argument that *Zha* fails to
14 disclose claim 28 sensitive information is shared only with the second
15 device.

16 Slide 45. Again, this argument fails because *Zha* expressly discloses
17 this. We just saw this quote at Exhibit 1004, column 19, lines 3 to 13. *Zha*
18 says, "The server may send a private message only to the cellphone without
19 sending the private message to the laptop computer or the desktop
20 computer." Patent Owner ignores this express disclosure and instead
21 suggests that other embodiments, where *Zha*'s system can be configured to
22 send private messages to other devices, somehow renders this express
23 disclosure meaningless or somehow teaches away from claim 28.

24 But Patent Owner's teaching away argument here and elsewhere
25 throughout its reply does not satisfy the legal test for teaching away, which
26 requires a reference to criticize, discredit, or otherwise discourage

1 investigation into the invention claim. That's from the Federal Circuit
2 *Galderma Laboratories* decision in 2013 and is quoted at Petitioner's
3 surreply at pages 5 and 6. Patent Owner appears to believe that a reference
4 disclosing alternatives somehow teaches away from a claim that uses only
5 one of the alternatives, but that's not the law. Accordingly, Patent Owner's
6 third argument should also be rejected.

7 Slide 46.

8 JUDGE MURPHY: Counselor, can we go back to that slide just for a
9 second, please?

10 MR. BANNER: Certainly.

11 JUDGE MURPHY: Okay. It says the server may send a private
12 message. It doesn't say the server is prohibited from sending a private
13 message to the first device with a non-cellphone device. Correct?

14 MR. BANNER: The language is "the server may send a private
15 message only to the cellphone without sending the private message to the
16 laptop computer or the desktop computer." So I think that's pretty clear that
17 when it's configured in this embodiment, private messages are only being
18 sent to the cellphone and not the other devices.

19 JUDGE MURPHY: Even though they're using the word "may" there?

20 MR. BANNER: Certainly, yeah.

21 JUDGE MURPHY: Okay. Okay. Thank you.

22 MR. BANNER: And I think that the word "may" just acknowledges
23 that *Zha* is a configurable system and in other embodiments it might be
24 configured a different way.

25 JUDGE MURPHY: So the user in *Zha* does not have the option of
26 having -- with this embodiment, the user does not have the option of sending

1 a private message to the laptop computer. The private message can only be -
2 - the private message interface, excuse me, can only be accessed on the
3 cellphone?

4 MR. BANNER: As it's configured here. I mean, I believe the user
5 has the option to reconfigure it at a later time if it so desires. But that's no
6 different than the '376 patent where the user can decide whether or not it
7 wants to use the cellphone as a security device.

8 JUDGE MURPHY: Well, let's look at claim 28. Does claim 28 say
9 that it must -- that you can only do this or does it say that there's an option
10 where you can send sensitive information only to the second device?

11 MR. BANNER: Claim 28, the language here on slide 45, says "the
12 second subset of information comprises sensitive information and the
13 sensitive information is only shared with the second device." However,
14 claim 28 is a comprising claim. So a system could have any other
15 functionality and still meet this as long as there's some point in time where
16 the sensitive information was only shared with the second device.

17 JUDGE MURPHY: Thank you.

18 MR. BANNER: So slide 46, the analogous art argument.

19 Let's go to slide 47. So *Zha* and other references like *Takahashi* and
20 *Tsushima* are properly considered as analogous art because they are in the
21 same field of endeavor.

22 Slide 48. The Board's preliminary guidance is correct that the field
23 of endeavor of the '376 patent is a system or method in which a user
24 interacts with "a first electronic device and a second electronic device
25 throughout the use of an online application." So that's what the original
26 claims of the '376 patent are directed to. That is the field of endeavor.

1 Slide 49. Now, Patent Owner relies on the *Airbus* case to argue that
2 the correct field of endeavor should be narrowed to systems or methods to
3 protect information where a user interacts with a first electronic device and a
4 second electronic device throughout the use of an online application. So
5 what Patent Owner has done is it's basically adopted the field of endeavor
6 that the Board enumerated in the preliminary guidance and has added the
7 words "to protect information."

8 I'm going to skip to slide 52 here. Getting close on time. So Patent
9 Owner's reliance on the *Airbus* case is misplaced. Patent Owner has
10 creatively added these non-limiting amendments to its claims in an attempt
11 to affect the Board's determination of what the field of the endeavor is. The
12 "protecting information," that's what they're trying to add into what the
13 Board has said the field of endeavor is, are added in these limitations that
14 were not present in the original claims and, as I discussed with claim -- in
15 the claim construction section of my presentation, are non-limiting.

16 Allowing a Patent Owner to change the field of endeavor and avoid
17 prior art that is spot-on through non-limiting amendments would encourage
18 mischief by patent holders faced with invalidating prior art and IPRs and
19 should not be allowed. The *Airbus* case did not have these same facts and,
20 therefore, the Board should reject Patent Owner's non-analogous argument
21 here.

22 I believe that covers the disputes related to the *Zha* grounds. If there
23 are no questions, I'll move to *Kling* and *Lim*.

24 JUDGE BARRETT: Counselor, it seems like you're tracking your
25 time pretty well. I have you at about nine and a half minutes left.

1 MR. BANNER: Okay. So slide 53. Notably, *Kling* and *Lim* are both
2 directed to protecting against malware and systems where a first electronic
3 device and a second electronic device are used with an online application.
4 And so, you know, regardless of the non-analogous art argument in respect
5 to *Zha* and *Takahashi* and the other art, *Kling* and *Lim* both expressly are
6 directed at security of systems, banking systems and other systems, to
7 protect against malware where you have two devices accessing a system.

8 So slide 54. As the Board may recall, *Kling* discloses an online
9 banking application. There's no dispute that *Kling* discloses the preamble of
10 claim 26, as well as the limitations 26[a] and 26[b].

11 Slide 55. So what are the disputes with respect to *Kling* and *Lim*?

12 Slide 60. Again, I'm going to summarize the Patent Owner
13 arguments and then I'll go through the evidence. Patent Owner makes six
14 main arguments with respect to *Kling* and *Lim*. The first argument Patent
15 Owner makes is that *Kling* fails to disclose claim 26[c] because *Kling*'s
16 mobile phone login is device specific and does not log into the banking
17 application. This argument ignores the Board's preliminary guidance and
18 *Kling*'s express disclosure that the mobile phone logs into the banking
19 application.

20 Slide 57. Patent Owner's second argument is that *Kling* plus *Lim*
21 fails to disclose claim 26[c] because *Lim* only discloses authenticating with
22 one device, the mobile phone. Again, Patent Owner ignores *Lim*'s express
23 teaching that both the user terminal and the mobile phone are authenticated
24 in the system.

25 Slide 58. The third argument Patent Owner makes is that *Kling* plus
26 *Lim* fails to disclose claim 26[c] because *Lim*'s authentication information is

1 device specific. Again, Patent Owner ignores *Lim*'s express teaching that the
2 authentication information is not device specific as *Lim* uses passwords,
3 biometric information, and other device independent authentication
4 information.

5 Slide 59. The fourth argument Patent Owner makes is that *Kling*
6 plus *Lim* fails to disclose claim 26[c] because *Lim* teaches away from a
7 combination with *Kling*. Patent Owner's teaching away argument does not,
8 again, satisfy the legal test for teaching away, which requires the reference
9 to criticize, discredit, or otherwise discourage investigation into the
10 invention claim.

11 Slide 60. The fifth argument Patent Owner makes is that *Kling* fails
12 to disclose the if and only if limitation of 26[d] and 41[e], which is waiting
13 to send the first subset of information until after both devices have been
14 authenticated. Petitioner's evidence shows a POSITA when modified *Kling*
15 based on *Lim*'s -- sorry, based on *Lim*'s teaching in one of two ways, and
16 Patent Owner fails to address the first modification, which is moving *Kling*'s
17 mobile device login steps earlier in time to coincide with the PC login steps.
18 For Petitioner's second modification, Patent Owner incorrectly argues that
19 only the mobile phone and *Lim* is authenticated, but *Lim* expressly discloses
20 both the mobile phone and the desktop are authenticated.

21 Slide 61. The sixth and final argument is -- that Patent Owner makes
22 is that *Kling* fails to disclose claim 28, sensitive information is only shared
23 with the second device. Patent Owner simply fails to address the evidence
24 on which Petitioner relies, which is evidence that shows that sensitive
25 information, which is the web transaction confirmation information, is only

1 sent to the second device, mobile phone -- the mobile phone. That's how
2 *Kling* works.

3 So let's look at the evidence for these arguments, starting with Patent
4 Owner's first argument that *Kling*'s mobile phone login is device specific
5 and does not log into the banking application. This, like the rest of Patent
6 Owner's arguments, simply ignores the teachings found in the prior art.

7 Slide 63. At page 15 of the preliminary guidance, the Board already
8 found that *Kling*'s password was application specific. Patent Owner doesn't
9 explain why the Board's finding is incorrect. In fact, it's not.

10 Slide 64. On the bottom right of this slide we have *Kling* paragraph
11 18. That's Exhibit 1023, where *Kling* discloses the user logging into the
12 bank server with the mobile device. *Kling* states, "Typically the user would
13 be prompted to log into the mobile device, ideally using a different password
14 than on the PC."

15 Now, Patent Owner and its expert argue that this statement indicates
16 the user is logging into their mobile device and not the banking application.
17 So according to Patent Owner and Dr. Traynor, this login is device specific.
18 In other words, they suggest that this mobile device login is the password
19 you would enter to unlock your cellphone.

20 Now *Kling* figure 4 dispels that myth, and that's on the left-hand side
21 of this slide. The mobile device login steps are annotated in green on this
22 slide and are steps 413 and 414. At step 414, the user enters login and
23 password on the secondary device, which is the mobile phone. Step 413 is
24 performed by the bank server, which is sending a secondary login message
25 to be displayed on the mobile phone. Patent Owner's argument that the user
26 is logging into the cellphone and not the banking application makes no sense

1 in view of this figure. The only reason the bank server would send a
2 secondary login message is to allow the user to log into the banking
3 application with their mobile phone in step 414. Patent Owner and Dr.
4 Traynor ignore this teaching, much like they do for the rest of the *Kling* and
5 *Lim* arguments they make. They are simply not credible.

6 Slide 65. Patent Owner's second argument is that *Lim* only discloses
7 authenticating with one device, the mobile phone. This, too, ignores *Lim*'s
8 teaching.

9 Slide 66. So *Lim* is Exhibit 1030, and at paragraph 77, *Lim* discloses
10 that once the success of the authentication has been notified by the
11 authentication information processing module 250, the service server 300
12 determines that the user terminal 50 has been successful in the
13 authentication, allows normal access, and provides a variety of services that
14 can be utilized by a login user. This passage confirms that the user terminal
15 50 is authenticated as well as the mobile phone. Patent Owner is simply
16 wrong about *Lim*.

17 Slide 67. This slide depicts the other disclosures from *Lim*, Exhibit
18 1030, that confirm both the mobile terminal 100 and the user terminal 50 are
19 authenticated with *Lim* system. At paragraph 29 on the left, *Lim* discloses
20 the user enters a user ID and password on the user terminal, and at
21 paragraphs 33 to 42 on the left, *Lim* discloses the steps the mobile device
22 takes to authenticate. So you have both of these terminals entering
23 authentication information.

24 Slide 68. On the left, paragraphs 28 to 29 in *Lim*, Exhibit 1030,
25 disclose using an identifier and password for authenticating with the user
26 terminal. On the right, paragraphs 38 through 41 in *Lim* disclose various

1 authentication information for authenticating the mobile terminal. These
2 include an ID and password, authentication number, and various biometric
3 information.

4 Slide 69. Based on *Lim*'s disclosure, a POSITA understands that
5 authentication information used on the user terminal can be different from
6 that used on the mobile device. Even where both are IDs and password, a
7 POSITA knows they could be different, at least based on *Kling*'s disclosure
8 that ideally they should be different. So the application information -- the
9 application specific authentication information in *Lim* checks all the boxes
10 and meets all of the requirements of claim 26[c]'s limitation. It's application
11 specific, not device specific, and there's different information used for the
12 different devices.

13 Slide 70. Patent Owner's third argument for *Kling* and *Lim* is that
14 *Lim*'s authentication information is device specific. That's incorrect. I think
15 I just went through that. In the interest of time, I'll just refer back to what I
16 just -- the evidence I just went through.

17 Let's see, Slide 74. Patent Owner's fourth argument for *Lim* is that
18 *Lim* teaches away from a combination with *Kling* and because *Lim* teaches
19 using device specific authentication information.

20 Slide 75. Once again, Patent Owner does not satisfy the legal test for
21 teaching away. It is true that *Lim* discloses the use of some device specific
22 authentication information in some instances, but those are merely
23 alternatives or additional steps in the authentication process. It doesn't
24 change the fact that the passwords, biometric information, such as iris
25 information or fingerprints, are used to authenticate. So -- and those are
26 device independent. So that is all the revised substitute claims require is

1 device independence. There's simply no teaching away here. There's just
2 alternatives that are listed, and that is not a teaching away.

3 Slide 76.

4 JUDGE BARRETT: Counselor, you're at your original 45 minutes.
5 You can continue.

6 MR. BANNER: I may take a few more minutes, Your Honor. I'm
7 nearly complete.

8 JUDGE BARRETT: That's fine.

9 MR. BANNER: Thank you. Slide 76. Patent Owner's fifth argument
10 is that the if and only if limitation is not met by *Kling*. Patent Owner argues
11 that *Kling* sends information to the first device, the user terminal, before the
12 mobile phone is authenticated. And while that may be an accurate
13 description of *Kling* on its own, it ignores that Petitioner relies on *Lim*'s
14 teaching to modify *Kling*.

15 So slide 77. At paragraph 77 of *Lim*, Exhibit 1030, *Lim* teaches that
16 the online services are provided only after the user terminal 50 has
17 authenticated. This follows the authentication of the mobile phone. So
18 *Lim*'s teaching is that both devices are authenticated before starting the
19 service or sending any information. As pointed out in Petitioner's opposition
20 to the revised motion to amend, Paper 27 at pages 22 and 23, *Lim*'s
21 authentication enhances security against malware on the user terminal, and
22 that's disclosed at Exhibit 1030, paragraphs 9 and 10.

23 Slide 78. So this slide shows the if and only if language from the
24 claims if you don't transmit the first subset to the first device or the second
25 subset to the second device until both the first and second devices are
26 determined to be accessible.

1 Slide 79. So Petitioner's evidence shows that a POSITA would
2 modify *Kling* based on *Lim*'s teaching by "moving *Kling*'s mobile device
3 login steps earlier in time to coincide with the PC login steps." This is the
4 testimony of Dr. Meldal, paragraph 134, Exhibit 1029. This evidence is
5 unrebutted.

6 Looking at *Kling*'s modified figure 4 on the right-hand side of slide
7 79, we see how a POSITA would modify *Kling* based on *Lim*. This figure
8 comes from Dr. Meldal, Exhibit 1029, paragraph 130. On the bottom left
9 corner of modified figure 4, we see *Kling* steps 1 through 5. According to
10 *Kling*, those steps occur sequentially in that order. Patent Owner argues that
11 because the transaction webpage information is sent to the user terminal at
12 step 2, which is before the phone authenticates in step 3, the if and only if
13 limitation is not met. But as we see in the modified figure above, *Lim*
14 teaches to do authentication of both devices before sending any transaction
15 webpage information. So step 3 is moved earlier in time above that green
16 line so that the mobile phone logs in before any transaction web page
17 information is sent.

18 Dr. Meldal explains that a POSITA would have a reasonable
19 expectation of success in making this modification because password
20 logging schemes were well known by 2014 and moving the phone login
21 earlier in the process would not at all affect *Kling*'s operation. That
22 explanation is Exhibit 1029, paragraphs 122 and 119 to 121.

23 For the interest of time, I will rely on our briefing for the remainder
24 arguments and I will reserve the rest of my time for rebuttal.

25 JUDGE BARRETT: Thank you. I show you with about 12 minutes
26 remaining.

1 MR. BANNER: Thank you, Your Honor.

2 MR. BENISEK: Thank you, Your Honors. Eric Benisek on behalf of
3 the Patent Owner. And Judge Barrett, I think I'd like to reserve 10 minutes
4 for surrebuttal if that's okay.

5 JUDGE BARRETT: Reserving 10 minutes. That's fine.

6 MR. BENISEK: Okay, great.

7 JUDGE BARRETT: You may begin whenever you're ready.

8 MR. BENISEK: Okay. I, too, will be presenting a screen share, so let
9 me get that going.

10 Okay. Good afternoon, Your Honors. I want to start, before I sort of
11 dive in and respond to the various arguments raised by Petitioner, I want to
12 give a little bit of background on the patent and the inventor for just a little
13 bit more context.

14 Dr. Rubin, who is on the line listening, is a recently retired professor
15 of computer science at Johns Hopkins and he's also the former technical
16 director at Johns Hopkins Information Security Institute. When Dr. Rubin --
17 basically Dr. Rubin spent his career at Johns Hopkins researching the field
18 of information security. And when he came up with the idea for the '376
19 patent, two factor authentication was the state of the art.

20 Common two factor authentication that we know from back then and
21 we know today is where you're on your PC, you go onto your browser, surf
22 over your bank, you attempt to log in, you have to enter a username and
23 password. That's the first authentication. Once you get past that, then the
24 bank sends a code to a second device. You have to then take that code that
25 was sent to your second device, enter it onto your first device, and then
26 you've performed the second factor of authentication. And that is sort of the

1 traditional two factor authentication, which was a state of the art at the time.
2 And it is a quite common way that banks still continue to authenticate.

3 JUDGE BARRETT: Mr. Benisek, you are sharing your screen. I'm
4 not sure if that's what you intended to share. Are you wanting to show your
5 demonstratives?

6 MR. BENISEK: Oh, I'm sorry, I did want to share. Thank you for
7 pointing that out, Your Honor. Hopefully you're seeing my cover slide now
8 for the demonstratives.

9 JUDGE BARRETT: Give us a moment. I'm not seeing anything just
10 yet. It's still working, I believe. All right, I'm seeing some demonstratives.
11 Are those yours?

12 MR. BENISEK: Yes.

13 JUDGE BARRETT: Yeah, we're good.

14 MR. BENISEK: Yeah. Okay, great. All right. Thank you, Your
15 Honor.

16 So as I was saying, two factor authentication has been an important
17 security measure to defeat malware, but it has its shortcomings, as described
18 in the '376 patent. Namely, if your first device is already infected with
19 malware, two factor authentication doesn't protect you from the malware
20 that is already on your device. And so anything you do on the first device
21 can be observed and captured by the malware.

22 So when Dr. Rubin conceived this idea, he was looking -- he sort of
23 conceived the idea that you could advance two factor authentication by
24 specifically designing online applications to simultaneously use both devices
25 and then only share the sensitive information with the second device. And
26 that would, one, keep all the benefits of two factor authentication, but also

1 add the extra benefit of not exposing the sensitive information to the first
2 device. That is the essence of the '376 patent.

3 And with that introduction, I'm going to move to a number of the
4 arguments raised by Petitioner, first being written description. And I'm just
5 going to actually use Petitioner's -- a couple of Petitioner's slides. They
6 would be just for reference, slides 10 and 12 for Petitioner. And this is
7 basically the argument that there's no written description support for limiting
8 the first device to non-device specific authentication information. And we
9 think that -- we sign our paperwork, which is the case law, which is negative
10 limitations are permissible and are supported when there is a specific
11 teaching as to why you would cause or claim the negative limitation. And
12 the teaching or the concept is basic, which is in order to be able to use
13 different devices, you don't want to use device specific authentication
14 information because that limits you to that device. That's the concept.

15 It's stated clearly in Dr. Rubin's specification in paragraph 92. And it
16 applies to any device. And that was the testimony of Dr. Traynor. He
17 explained that that concept is known to a POSITA. It applies to any device
18 that you're going to use, first, second, third, whatever.

19 And also, I'll just note, as we noted in our papers, that Dr. Rubin
20 specifically says in the patent that the idea here, it's paragraph 19 of Exhibit
21 2005, is that you should be able to use any device, and that's -- as first and
22 second. And so not only is Dr. Rubin teaching that this invention you
23 should be able to use any combination of devices, but then he teaches the
24 concept that, and if you want to make sure you can use any device, make
25 sure not to use device specific authentication information in the
26 authentication process.

1 So we think that's the reasoning. It applies to all the devices and that
2 provides the written description support for this added limitation.

3 Plaintiff's second -- I'm sorry, Petitioner's second written description
4 argument is that the added limitation sensitive information only shared with
5 the second device, which is specific to claim 28, is not supported. And that's
6 referred in slides 14 and 15 of Petitioner's presentation. There's the
7 language. We think that there's more than ample support for this.

8 We'll take the poker embodiment. I think Petitioner's complaint
9 about the poker embodiment is that the hole cards are eventually shared with
10 the first device. But throughout Dr. Rubin's specification, he explains that
11 the hole cards are no longer sensitive information at that time, which is
12 completely consistent with this Court's definition of sensitive information,
13 which is sensitive, proprietary, and confidential, and shouldn't be shared
14 with others. But at the point the game's over, that information is no longer
15 sensitive. I think anyone wouldn't debate that on this call. And at that time
16 it's shared with the first device and the specification teaches that.

17 I will say that the argument that all of the embodiments require
18 sensitive information to be shared beyond the second device is just not true.
19 If you look at the other embodiments, the non-poker embodiments, banking,
20 healthcare, managing your brokerage accounts, banking is at paragraphs 56
21 through 60 of Exhibit 2005, healthcare is 77 through 78, and brokerage
22 account is 63. All of those embodiments disclose sending the information
23 just to the second device and not sharing it beyond the second device. So
24 I'm sort of perplexed at how those embodiments somehow are contrary to
25 this particular claim limitation.

1 Okay. I'm going to move to claim construction next. And this is
2 going to be slide 2 of Patent Owners demonstratives. It's our position that
3 the thereby clause is limiting. It was specifically inserted to be limiting.
4 That was certainly Dr. Rubin's intent. There's no intent at mischief here as
5 being suggested by Petitioner.

6 The test -- well, the *Hoffer v. Microsoft* case, which is cited in our
7 papers, states whereby clauses "generally state the result of a patented
8 process," but "when the whereby clause states a condition that is material to
9 patentability," it is limiting. And that's exactly what we set out to do with
10 this limitation. And the point here is it's not enough to perform all the steps
11 of claim 26 and you magically infringe, whether the information is protected
12 or not. The information actually has to be protected. Dr. Traynor explained
13 this. He testified to this and he explained that by segregating the
14 information sent to the two devices, you are creating isolation of the
15 information.

16 But what Petitioner didn't tell you is that he went on to explain that
17 that isolation actually has to exist. If you send the information to the two
18 devices and the first device has full access to everything on the second
19 device, then there's no isolation and there's no protection. So we feel that
20 this limitation is actually extremely material to patentability because without
21 it, you would be sort of technically infringing the patent in the sense that you
22 might practice the steps, but your information is not protected. So that was
23 certainly the intent of this limitation. We think it fits squarely within *Hoffer*
24 *v. Microsoft*.

25 And I'll just note, I think *Hoffer v. Microsoft* is a good case to look
26 at. The posture was opposite of what it is here in the sense that there the

1 Patent Owner was trying to get out of a whereby clause by claiming it wasn't
2 limiting and that in that particular case, the whereby clause required the
3 users to be able to interactively message each other. And the Patent Owner
4 said, hey, it's a whereby clause, the patent doesn't actually have to -- or the
5 accused device doesn't actually have to allow you to interactively message.
6 And there the Court and Federal Circuit said, well, no, that is the point of the
7 invention is that you're supposed to be able to do this once you've done these
8 steps. And that's exactly what we're saying here. It would be sort of the
9 akin, if Dr. Rubin was Mr. Hoffer, he would be arguing, oh, you performed
10 all my steps, but the information is protected, you still infringe.

11 So that's our position on the whereby clause. We think it's absolutely
12 limiting and we think that that also informs the field of endeavor, which I'll -
13 - and (inaudible), which I'll talk about in a little bit.

14 JUDGE CHERRY: Mr. Benisek, I guess I just wanted to push back a
15 little bit because, I mean, I feel like we're in a different situation than in
16 *Hoffer*. I mean, here these claims haven't been issued. I mean, it's because it
17 seems like in prosecution -- I mean, this seems more akin to prosecution. I
18 mean, then every whereby clause or thereby clause that an applicant adds in
19 a patent application would then be a limitation. I don't think that they're
20 treated that way. Can you give me a little bit of help there?

21 MR. BENISEK: Well, I think, Judge Cherry, I think that the *Hoffer*-
22 *Microsoft* case, it acknowledges that whereby clauses generally state the
23 result of a patented process. And if that's it, then it's non-limiting. But I
24 think we're different here because you can practice the steps, but there is -
25 which I'm going to get into when I talk about the other references, but there's
26 a very easy way to end up where the information is not protected, and thus

1 you're missing the key aspect of the invention, which is to actually protect
2 the information that you've isolated from the two devices. And so we think
3 that falls squarely within the *Hoffer-Microsoft* situation, where it's a
4 condition, the protecting the information is a condition that is material to the
5 patentability. Okay.

6 JUDGE MURPHY: Counselor, I'm going to ask you to sort of, and I
7 apologize, I'm going to ask you to sort of baby talk me through here, what's
8 happening with the different sets of information, because I seem to hear you
9 arguing that if the user can bring the second information onto their first
10 device, then there's no protection. In other words, if the user decides I'm
11 going to use the first device for this and the second device for this to keep
12 things safe, that would protect the information. Do I understand you arguing
13 that this claim limitation says the user cannot possibly bring it over to the
14 first device, it can only go to the second device?

15 MR. BENISEK: Your Honor, I think what we're arguing is that the
16 system is with -- take the poker example, and I can also take the banking
17 example, which is the system is set up to send two different sets of
18 information to the two different devices, and that is that sort of application
19 designed by whoever created the application.

20 JUDGE MURPHY: So this is happening at the server, at the game
21 server, correct?

22 MR. BENISEK: It's happening at the game server. The game server -
23 -

24 JUDGE MURPHY: Okay.

25 MR. BENISEK: The game server application -- or I should say the
26 application running on the game server is making a determination of what

1 information to send to the first device and what information to send to the
2 second device. And with claim 28 in particular, it's the sensitive information
3 that is being sent to the second device and not any other devices.

4 And when we say not shared, that's the idea of it's not shared with
5 the first device or other devices. And that's not -- when I think about it or
6 when we think about it, we don't think about it as the user. We think about
7 as the system not sharing it with other devices. And we think that *Zha* and
8 *Takahashi* actually do share and hence they don't meet this claim limitation.

9 But does that answer your question?

10 JUDGE MURPHY: Well, I'm looking at the claim limitation here
11 that you have up on the screen or whatever we want to call it here, and it
12 says, "thereby protecting the second subset of information not transmitted to
13 the first device from potential malware on the first device." And it seems to
14 me this would cover a scenario where the game server is capable of sending
15 it to either device, but the user decides I'm only going to send the sensitive
16 information to my second device, e.g., my cellphone, and I'm going to send
17 the non-sensitive information to my computer. To me, this clause covers
18 that scenario. And correct me if I'm wrong, I'm looking for where in here it
19 says --

20 MR. BENISEK: Well, I guess I would go back to -- it's not here in
21 28. I would pull back to claim 26, the independent claim where --

22 JUDGE MURPHY: Can we go back there? Yeah.

23 MR. BENISEK: I'm sorry?

24 JUDGE MURPHY: Can we go back to the -- are you saying there's
25 claim language in independent claim 26 that covers that?

26 MR. BENISEK: Yeah.

1 JUDGE MURPHY: That precludes that? Yeah.

2 MR. BENISEK: Yeah.

3 JUDGE MURPHY: Let's go back and look at that because I think
4 this is an important point.

5 MR. BENISEK: So hopefully you can see my screen.

6 JUDGE MURPHY: It's fine. Yes.

7 MR. BENISEK: Yeah. And the idea is that you have information
8 being stored at the server.

9 JUDGE MURPHY: Mm-hmm. And that includes the first set of
10 information, the first subset, the second subset, the authentication
11 information. Is that what the information that the server is referring to right
12 there in limitation 26[a]?

13 MR. BENISEK: It is I think just referring, you know, generally to
14 sort of like the entire application information.

15 JUDGE MURPHY: Okay. Okay.

16 MR. BENISEK: But it gets narrowed. I think that's just the broad
17 statement, information at the server. And then when we go to 26[b],
18 identifying the first set -- subset of "the" information, and so now we're
19 drawing a first subset from the information stored on the server and then
20 we're also identifying a second set of "the" information that was stored on
21 the server. And then these two subsets are generated by the same
22 application. So your banking application has --

23 JUDGE MURPHY: Okay.

24 MR. BENISEK: -- generated these two subsets at the server and
25 they're specific to that application. And then 26[c] really just talks about the
26 authentication process, like how are we going to authenticate the two

1 devices? And then when we go to 26[d], this is the if and only if we
2 successfully authenticate above, do we then transmit the -- transmitting the
3 first subset of information to the first device from the server and transmitting
4 the second subset of information to the second device from the server.

5 JUDGE MURPHY: Now does that say authenticating or does that say
6 that they both have to be authenticated or does that say that they have to be
7 accessible?

8 MR. BENISEK: It says that, up in 26[c], that both devices need to be
9 authenticated --

10 JUDGE MURPHY: Okay.

11 MR. BENISEK: -- before you get to 26[d], before you can send the
12 information.

13 JUDGE MURPHY: Okay.

14 MR. BENISEK: And so -- yeah.

15 JUDGE MURPHY: Okay. I'm sorry, I interrupted you. Go on.

16 MR. BENISEK: Oh, no, no, that's fine, Your Honor. I expected to be
17 interrupted throughout.

18 So when you go to 28, and we're looking at the -- adding this
19 limitation, the second subset of information which has drawn from the
20 application, basically what we've done in 28[b] is specify that that second
21 subset of information comprises sensitive information and it is only shared
22 with the second device. And so that is thoroughly consistent with the poker
23 example because the only time that the hole cards are shared is when the
24 game's over and they're no longer sensitive. And then we --

1 JUDGE MURPHY: So the second subset of information is sensitive,
2 but then it becomes non-sensitive, and at that point it can be conveyed to the
3 first electronic device?

4 MR. BENISEK: Absolutely. That would be consistent with claim 28
5 in the sense that it's only been shared with the first device after it's no longer
6 sensitive information.

7 JUDGE MURPHY: But it's still the second subset of information,
8 correct?

9 MR. BENISEK: Yes. Yes, it is.

10 JUDGE MURPHY: Okay.

11 MR. BENISEK: It's a portion. It's at least a portion of the second
12 subset of information.

13 JUDGE MURPHY: Okay.

14 MR. BENISEK: Yes. Okay.

15 JUDGE MURPHY: So let's look at that, 28[b]. Can we go back? I'm
16 sorry.

17 MR. BENISEK: No, that's fine.

18 JUDGE MURPHY: I should quit apologizing. The 28[b], it says --
19 but it says the second set of information, the second subset of information.
20 But what you're saying is the second subset of information includes those
21 hole cards that are eventually shared with the first device, right, in the poker
22 example?

23 MR. BENISEK: In the poker example, the hole cards are the sensitive
24 information. They, you know, may or may not comprise all of the second
25 subset of information as this is just a comprising -- information comprises --
26 the second subset of information comprises sensitive information, and the

1 sensitive information is only shared with the second device. So at least
2 amongst the second subset of information, whatever is sensitive is not shared
3 with the second device -- the first device, excuse me.

4 JUDGE MURPHY: Do we have a definition of what is sensitive in
5 the specification?

6 MR. BENISEK: We don't specifically, Your Honor. I think in the
7 preliminary guidance, the Board cited sort of some publicly available sort of
8 dictionary definitions --

9 JUDGE MURPHY: Okay.

10 MR. BENISEK: -- that I think both parties were okay with.
11 Generally speaking, it made sense and so we were going to go -- I mean,
12 Petitioner can respond, but we were fine with the Board's definition and
13 preliminary guidance.

14 JUDGE MURPHY: Okay, thank you.

15 MR. BENISEK: Yeah, you're welcome.

16 Okay. Well, I think I've covered the *Kling* construction issues I
17 wanted to cover. I wanted to move next to the *Kling* reference in
18 combination or -- yeah, in combination with *Lim*. Okay.

19 JUDGE MURPHY: Can we touch on the analogous art just for a
20 second before we move on to *Kling*?

21 MR. BENISEK: Absolutely.

22 JUDGE MURPHY: Yeah. Okay. Here's my question. You know, I
23 understand you saying that the field of the endeavor here is the security, you
24 know, the protection of the information. But when I'm looking at the issued
25 claims, they don't seem to touch on that. Are you saying that your field of
26 endeavor has changed now that your claims have changed? Because I'm

1 looking at issued claim 1, and we don't have any of the authentication in
2 there. We don't have any of the, you know, the protection that you're talking
3 about now in the thereby clause.

4 MR. BENISEK: Yeah. No, absolutely. So how I would describe the
5 initially filed claims is that claim 26, or I guess original claim 1, if you read
6 it in the abstract without reference to the specification, it could be construed
7 more broadly to seem to refer to architecture of the claim. I think when you
8 read it in light of the specification, there's zero way that you could not
9 understand that independent claim 1 was directed towards security.

10 I think claim 3, now claim 28, includes the sensitive information
11 limitation, which is very security-oriented in the sense that now you're not
12 just talking about architecture of the invention, but you're actually directing
13 the sensitive information to one of the two devices. And so we absolutely
14 believe that claim 21 -- claim 3, now claim 28, out of the gate disclosed the
15 security in the claim itself, and then as well as the security specification.

16 JUDGE MURPHY: So by claim differentiation, then your original
17 issued claim 1 would have covered also non-sensitive information, correct?

18 MR. BENISEK: Yes, Your Honor.

19 JUDGE MURPHY: It wouldn't have to be sensitive and non-
20 sensitive. Okay, thank you.

21 MR. BENISEK: That's right. Okay. And I'd happy to stay on
22 analogous art.

23 JUDGE MURPHY: Well, continue with your flow. Continue with
24 your flow.

25 MR. BENISEK: Okay. Okay, great. All right. So back to *Kling* and
26 *Lim*. I wanted to deal with *Kling* and *Lim* first, because, frankly, I think it's

1 the easiest reference to deal with. And the main issue with *Kling*, which I
2 don't think is disputed, but it is the fact that *Kling* does not disclose the if
3 and only if limitation. And I'll back up a little bit on *Kling*.

4 *Kling* was -- or I should say, we have no debate or no dispute that
5 *Kling* is analogous art. *Kling*'s two factor authentication. It's -- and
6 definitely in the same field of endeavor. It's definitely trying to solve the
7 same problem. The only issue is we feel it's prior art, and we feel that, you
8 know, it was actually cited by Dr. Rubin to the Patent Office as prior art.
9 And I think the Patent Office didn't consider it mainly because *Kling* was
10 missing -- or one big reason was that *Kling* was missing the if and only if
11 aspect to the claims, which is important.

12 So in light of that, the Petitioner has to modify the claim in order to
13 meet the limitations of the patent invention. And they've chosen to do that
14 with *Lim*. And we have an absolute fundamental disagreement about what
15 *Lim* discloses. And we think we're right and I'm going to walk you through
16 it. And because of this difference, we think that, you know, any sort of
17 attempt to combine *Lim* with *Kling* fails, and *Kling* can't disclose -- fails to
18 disclose all the limitations because it fails to disclose the if and only if.

19 So, actually, this is more of the punchline. So I want to kind of walk
20 you through what our dispute is. But basically what our dispute is, is that
21 Petitioner has taking the position that both devices disclosed in *Lim*
22 authenticate with the server. So they both log in with a username and
23 password and they both authenticate and hence they disclose that limitation.
24 What I'm going to show you is that *Lim* actually only discloses
25 authenticating with one device, the mobile device. And it expressly says in

1 the plainest language that the first device does not authenticate. And I'm
2 going to show you that.

3 So what I'm putting up on the screen for you is the *Lim* patent. It's
4 Exhibit 1030. And what I've done is I've split the screen. I've got the
5 columns on my right and the figures on my left. And I'm just really going to
6 talk about figure 1, because that's all we really need to talk about. And so
7 what -- actually, sorry, I'm going to just jump around a bit because I just
8 want Petitioner's argument to be really clear. It's Petitioner slides 68 through
9 70. Wish there was a quicker way I could get there. Here we go. I think
10 frame it well, at least what their position is.

11 So down here in the bottom, Petitioner is arguing terminal 50, the
12 user enters an ID and password via authentication interface displayed in user
13 terminal 50. A user does not do that. I will show you that that actually does
14 not happen. They repeat that argument here, oops, suggesting that the user
15 enters an ID and a password for terminal 50. That does not happen. What
16 the user does is the mobile device enters the ID and the password. And I
17 believe they repeat it here, user terminal 50 authenticates.

18 Now, this is critical because they are claiming that *Lim* discloses this
19 dual device authentication, and that fills the claim gap. But *Lim* doesn't
20 disclose that.

21 So when we go to *Lim*, what Petitioner is rely on is this, paragraph
22 28. See if I can make it big for you. And it's referring to the initial step here
23 of 50 reaching out to server 300. And I can read it for you, but the key here
24 is when 50 reaches out to server 300, it gets back an authentication interface.
25 And that authentication interface is a little circle that you see over in figure
26 1. And it has three things in it. It has a barcode, and then it has two entry

1 bars for an ID and a password. And what 28 and 29 don't say is that the user
2 at 50 enters a password and a username and logs in. And, in fact, it says the
3 opposite if you keep going.

4 And so what it says is, as you sort of roll through this column,
5 starting 28, 29, 30, I'll kind of get to the important part. Yeah. And so when
6 you go to paragraph 33, once the authentication interface included the
7 identifier 60 has been displayed on the monitor via user terminal, the user
8 captures the identifier 60 using the mobile terminal 100 and may send the
9 captured identifier to system 200. And so what happens is there's no logging
10 in here at 50. The mobile device takes a snapshot of this interface and then
11 sends that barcode to the server 20 over here. And then server 20 checks
12 with server 300 if that is indeed the barcode that is sent. And that is
13 discussed specifically in these paragraphs: paragraphs 34, 35, 36, and 37.

14 And let's see. Yeah. And then finally, when you get to paragraph
15 38, I've highlighted the language here. It says, after the mobile device has
16 checked in and confirmed the barcode is accurate, it says, "Thereafter it is
17 determined that the identifier information is valid. The authentication
18 system 200 requests the authentication information from the mobile
19 terminal. The mobile terminal 100 provides authentication information to
20 the authentication system, thereby performing the final authentication
21 process." And then it describes what kind of passwords you can use.

22 But here's the key. Okay, this is the punchline, the headline,
23 paragraph 43 and 44. And after describing that whole process, it says, "That
24 is, in the present invention, the user terminal 50 itself will connect with --
25 excuse me, the user terminal 50 itself that will connect with the service
26 server 300 does not perform authentication. In the present invention, the

1 user terminal 50 only displays an identifier on the monitor screen in the
2 authentication process, but does not become a principal agent of the
3 authentication." That cannot be a more clear statement that what you see in
4 figure 1 is device 50 starting a process, but then the authentication being
5 carried out by the mobile device. And in light of that, that is just sort of
6 directly opposite to how Petitioner is characterizing this reference. In light
7 of that, we don't think --

8 JUDGE MURPHY: Counselor, are you saying that -- I'm looking
9 there at figure 1. I have to lean close, I have very old eyes. That
10 authentication, that the user doesn't have to put in any authentication to get
11 the ball rolling? He just logs on, no password, no application, and he goes
12 right to that server?

13 MR. BENISEK: Absolutely. In paragraph 28 and 29, they describe
14 that the user makes contact with the server, they start the authentication
15 process, and they get this authentication interface immediately back and then
16 proceed with the whole process that you see. And then if there's any doubt
17 that 50 -- whether 50 authenticated or not, it's stated in paragraphs 43 and 44
18 where it says there was no authentication done by the user at 50. So that is
19 absolutely our position on that.

20 JUDGE MURPHY: Can you bring up paragraphs 43 and 44 again for
21 me?

22 MR. BENISEK: Yes.

23 JUDGE MURPHY: Because that seems --

24 MR. BENISEK: Can you see that okay?

25 JUDGE MURPHY: I can. I can.

26 MR. BENISEK: Okay.

1 JUDGE MURPHY: Okay. That seems to me that it's saying that the
2 authentication is performed by the server, not the user terminal. Explain to
3 me why I'm reading that wrong.

4 MR. BENISEK: I'm not sure. I just -- reading this and consistent
5 with Dr. Traynor that it's saying specifically that terminal 50 that will
6 connect with the server service 300 does not perform the authentication.
7 And then it goes on to say terminal 50 only displays an identifier on the
8 monitor screen in the authentication process. That's exactly what we're
9 saying. All it does is display the authentication interface, which is
10 subsequently captured by the mobile phone. Ultimately, it goes around and
11 authentication occurs at 300. But remember, the claims require a first and
12 second device to authenticate with their own non-device specific
13 authentication information simultaneously. And that's just not what we have
14 here. We have one device doing the authentication, the mobile device, and
15 then the rest is performed by the server.

16 JUDGE MURPHY: Okay, thank you.

17 MR. BENISEK: You're welcome. So we have other issues with
18 *Kling*. They're briefed in our papers, but I don't think we really need to
19 belabor them because it's our view that this is dispositive and lack of the
20 missing if and only if and the lack at *Lim* is just completely deficient in
21 filling that piece.

22 I know Petitioner takes the position that we didn't dispute one of the
23 two modifications of *Kling*, but that sort of misunderstands our opposition.
24 Our opposition is that *Lim* doesn't say what Petitioner says it says in the
25 sense of two -- a system using two devices that authenticate independently
26 with their own password -- usernames and passwords, or, you know,

1 application specific authentication information that is not device specific.
2 You don't have two devices doing that with *Lim*. Therefore, you can modify
3 *Kling* all you want. *Lim* isn't giving you the guidance to do that.

4 JUDGE BARRETT: Counselor, you have about nine and a half
5 minutes left.

6 MR. BENISEK: Thank you. Okay. I'm going to move to analogous
7 art.

8 Okay. So this is starting slide 4 of the Patent Owner's
9 demonstratives, and we think it would be error to find *Zha*, *Takahashi*, and
10 *Tsushima* analogous art. I believe where we are in agreement in reviewing
11 Petitioner's slides on the test of analogous art. And I also think that there's
12 not really a dispute about the second part of the test, or at least there's not
13 really an argument, but I'll get into it.

14 And so we talked about field of endeavor, two separate tests. And
15 so, you know, whether the art is from the same field of endeavor, regardless
16 of the problem it addresses, it's analogous. We get that. And then the
17 second test is, if the reference is not within the field of the inventor's
18 endeavor, whether the reference is still reasonably pertinent to the particular
19 problem in which the inventor is involved and not. So I'll just shorthand that
20 for the reasonably pertinent test.

21 So starting with the field of endeavor discussion. To determine the
22 field of endeavor, the Board, this is spelled out in the *Airbus* case, the Board
23 should consider explanations of the invention's subject matter in the patent
24 application, including the embodiments, function, structure of the claim --
25 and structure of the claimed invention.

1 When we go on to slide 5, these are the things that the *Airbus* case --
2 the Board in *Airbus* and, ultimately, the Federal Circuit in *Airbus*
3 considered. It looked at the written description and it looked at the claims,
4 and when it looked at those things, it looked at the preamble of claim 1, and
5 it saw "a system for providing breathable fire prevention and suppression.
6 When it looked at the title of the patent, it's "Hypoxic Fire Prevention and
7 Suppression." When I looked at the specification and saw over and over
8 again, specification "indisputably is directed towards the problem of fire
9 prevention," which leads to kind of a not shocking conclusion that the
10 challenged claims were expressly directed to fire prevention and fire
11 suppression. Okay.

12 When you take those same factors that the *Airbus* Court looked at,
13 and you look at them with the '376 patent, that the evidence is even stronger
14 for our position of what the field of endeavor is. You start with the
15 preamble of all the claims, a method for protecting information. All the
16 claims now require that, thereby protecting the second subset of information.
17 Now, remember, we claim that these are limiting.

18 The title of the patent, "Utilization of Multiple Devices to Secure
19 Online Transactions." The abstract the inventions defined "can be
20 configured for securing communications against malware." Field of
21 invention, "securing communications against malware." And finally, the
22 detailed description, "prevent a compromise of a transaction if malware
23 infects either device." To us, it's sort of overwhelming that these challenged
24 claims are directed towards security and protecting information with two
25 devices during online application. I mean --

1 JUDGE MURPHY: Counselor, can we look at the preamble here for
2 a second?

3 MR. BENISEK: Mm-hmm.

4 JUDGE MURPHY: It says, "A method of protecting information."
5 What is the -- is that information -- it's not all the information, right? It's just
6 the second subset of information, correct?

7 MR. BENISEK: Absolutely. In the preamble. That's right.

8 JUDGE MURPHY: Okay.

9 MR. BENISEK: Yeah. So we feel that that's starting with that
10 because that's really step 1. What is the field of endeavor? And you follow
11 *Airbus* and you look at these variables, and that's where we believe the
12 Board should land. But now we have to look at the actual references to see
13 where they land.

14 And so taking the '376 field of endeavor compared to the cited prior
15 art, before I sort of walk through these, I think *Airbus* is useful. It has a very
16 useful quote in figure -- in footnote 8, which notes that the Court sort of
17 states the obvious, which is like, hey, when you look at these prior art
18 references, you can look at the field of invention and it gives you a pretty
19 succinct summary of what the field of endeavor is. And so that in part is
20 baked into what I have on the slide, but it's also applying *Airbus* factors.

21 When you look at *Zha*, its field of invention, and I think sort of
22 indisputably its disclosure relates to a method for displaying interface, an
23 apparatus terminal and server, and we'll get into all, you know, the field,
24 that's the field. And then the problem it's trying to solve is to improve, you
25 know, bandwidth usage and user switching costs.

1 When we look at *Takahashi*, you know, *Takahashi* explains its field
2 of endeavor as a technique for controlling game progress with the
3 communication terminal of a user of our communication network.

4 *Tsushima* is even maybe the most far field and that presents an
5 invention relating to content providing system, a control method thereof, and
6 particularly to a streaming distribution technique for encoded video data.

7 And then finally *Kling*. This invention relates generally to the field
8 of online transaction security. That's the field of endeavor we think is
9 appropriate and are not disputing.

10 But there's a second test. There's the reasonably pertinent test that
11 these references could fall into as well and still be considered analogous
12 prior art. Now, I guess my point here is that Petitioner hasn't made the
13 argument that these references are reasonably pertinent. I hear the Petitioner
14 making the argument that they're in the same field of endeavor, which we
15 dispute. We think it's sort of not possible to claim these references are
16 reasonably pertinent to the problem that the inventor, Dr. Rubin, was trying
17 to solve in our case.

18 Here is the test. I think this language highlighted here is key. "In
19 other words, references are reasonably pertinent only if a person of ordinary
20 skill in the art would reasonably have consulted those references and applied
21 their teachings in seeking a solution to the problem that the inventor was
22 attempting to solve." And that's from *Airbus*.

23 When we go to these references -- now, to be clear, in the Board's
24 preliminary guidance, they sort of took issue with Patent Owner's arguing
25 that these references had to be solving the same problem. And we're not
26 arguing that. We are following *Airbus* to the letter, which is our position is

1 nothing in these references would lead a POSITA to follow their teachings
2 to solve the problem in the '376.

3 Now, what was the problem in the '376? It's kind of stated all over
4 the reference, but we sort of summarize it up here. It's prevent the
5 compromise of an online transaction by malware. Pretty simple. That is the
6 goal. And when you look at what *Zha* was trying to do --

7 JUDGE MURPHY: Counselor, it says, "to prevent the compromise
8 of an online transaction by malware." Is the healthcare and the health
9 information and the poker game, is that considered an online transaction?

10 MR. BENISEK: Absolutely. Yeah, I think it's -- yes.

11 JUDGE MURPHY: Okay, thank you.

12 MR. BENISEK: Yeah. So I think, I mean, we've sort of summarized
13 the problems that *Zha*, *Takahashi*, *Tsushima*, and *Kling* were all attempting
14 to address, and their teachings are directed at trying to solve those problems.
15 We obviously don't dispute that *Kling* -- the teachings of *Kling* would be
16 relevant to trying to solve the same problem that Dr. Rubin was trying to
17 solve. So we think *Kling*'s analogous art under either test. But we believe
18 that *Zha*, *Takahashi*, and *Tsushima* are just too far afield. And frankly, there
19 hasn't been any teaching identified by Petitioner that would drive Dr. Rubin
20 to have gone and looked at those references to come up with his invention of
21 using the two separate devices simultaneously to protect the second subset of
22 information.

23 JUDGE BARRETT: Counselor, you're eating into your rebuttal time
24 now.

25 MR. BENISEK: Oh, thank you. Let me check. Thank you, Your
26 Honor. How much rebuttal time do I have now?

1 JUDGE BARRETT: I'll give you your full 10 minutes if you're going
2 to stop now.

3 MR. BENISEK: Okay, excellent. I'll stop now and I'll circle back.
4 Thank you.

5 JUDGE BARRETT: Okay. Petitioner, I have you down for 12
6 minutes remaining.

7 MR. BANNER: Thank you, Your Honor. Let me share my screen
8 here. And let me -- can you see my screen at this point?

9 JUDGE BARRETT: Yes.

10 MR. BANNER: Okay, great. May it please the Court. Thank you
11 again for this opportunity. I do want to take three issues that were raised in
12 the Patent Owner's presentation. Kind of do it in reverse order, I think, from
13 what was just discussed, and start with analogous art, then talk about the
14 claim reference, and then go to the claim construction.

15 So this is slide 48 of Petitioner's presentation, and it's a quote from
16 the preliminary guidance, Paper 21 at 17 and 18 and 24 and 25, where the
17 Board preliminarily told us what the field of endeavor of the claimed
18 invention is, which is a first electronic device and a second electronic device
19 -- I'm sorry, "a system or method in which a user interacts with a first
20 electronic device and a second electronic device throughout the use of an
21 online application." We believe that's correct.

22 What happened here is that the Patentee, while, you know, having
23 some language in the title and maybe the abstract and elsewhere in its
24 specification about protecting against malware or having security concerns,
25 the Patentee sought and obtained claims that are broader than those ideas of
26 protecting against malware and obtaining security. Claim 1 of the original

1 patent that issued does not mention malware, does not mention security. It is
2 much broader and is simply targeted at different transmission of data to
3 different devices, where you have multiple devices accessing the same
4 application. That is what the Patentee sought and obtained. And that, as we
5 went into this IPR, is what the Petitioner had to look at, it's what the Board
6 looked at in its preliminary guidance, saying, that's what the broadest claims
7 are and that's the field of endeavor. To try to limit the field of endeavor to
8 some dependent claim, like Patent Owner has argued simply, is not -- there's
9 no law that would support that.

10 The Board is absolutely correct in this preliminary guidance to rely
11 on that broad claim, the original claim 1, to define the field of endeavor.
12 And so we believe that that's correct, and we believe that with that field of
13 endeavor, *Zha*, *Takahashi*, *Tsushima*, all the references that were raised in
14 the petition in response to the motions to amend are all within that field of
15 endeavor because they all also relate to systems and methods where a user
16 interacts with a first electronic device and a second electronic device
17 throughout the use of the online application.

18 So we believe that the analogous art the Board should find -- should
19 stick to its preliminary guidance in finding the scope of the prior art, and that
20 would render all of the claims unpatentable under all the grounds that were
21 raised. Even if the Board decides to change its mind, as Patent Owner has
22 conceded, *Kling* and *Lim* are within the field of security and protecting
23 against malware. So I'd like to move to the arguments that Patent Owner
24 made on *Kling*.

25 Now, going to go to slide 68 of my presentation. We heard a lot of
26 attorney argument with respect to what *Lim* shows or does not show. And I

1 don't think if you go and look at the evidence, if you go and look at what Dr.
2 Traynor said, a lot of what Mr. Benisek has argued today is simply not found
3 in that evidence, in that declaration. But I think that more fundamentally,
4 there is a misunderstanding of *Lim*. And if we look here on slide 68, again
5 on the left, paragraphs 28 and 29 of *Lim*, they talk about the user -- it says
6 when the user -- this is paragraph 28 of Exhibit 1030, "Referring to figure 1,
7 in an authentication method, according to the present invention, when the
8 user terminal 50 connects with the service server 300 and performs
9 authentication, for example, performs login. The service server 300
10 provides an authentication interface, including an identifier to the user
11 terminal 50." This paragraph says explicitly, the user performs login using
12 the user terminal 50. I don't understand how Patent Owner just glosses over
13 this, that somehow the system knows who the user is without the user
14 entering any identification information or any password information. I
15 mean, that simply doesn't make any sense.

16 The user is sitting there. And we can go back to slide 67 where we
17 see figure 1. The user is sitting there on a desktop computer labeled 50.
18 And that is what that paragraph 28 is talking about. The user first performs
19 login to the server -- service server 300, and says, hey, I'm Brian Banner. I
20 want to access my bank account. And in response, what the service server
21 does is it sends back that page that has the barcode and the other information
22 that then the cellphone uses, the mobile terminal uses to verify that I am who
23 I say I am. That's the whole point of *Lim*. And the whole point of *Lim* is
24 that both I have to log in first, and then I have to verify that login with my
25 cellphone before *Lim* will even start the application.

1 And we could -- we see that this is described by Dr. Meldal. He
2 goes through extensive discussion of the process that *Lim* takes. I can show
3 you that at -- let's get his -- you can see this. This is Exhibit 1029, Dr.
4 Meldal's declaration. And I can point you to paragraph 69 and the
5 surrounding paragraphs, where Dr. Meldal provides a flowchart of *Lim*'s
6 operation. We see over here on the right, performs -- the user terminal. It
7 performs login here on the left-hand side, in that second box on the left-hand
8 side under User Terminal.

9 So this idea that Patent Owner is coming in here and trying to tell
10 you that this is a one device authentication, that it's only the mobile terminal,
11 is simply unfounded. They pointed to, let me see, 43 and 44 of *Lim*, and this
12 is Exhibit 1030. And they said that this demonstrates that *Lim*'s user
13 terminal is not involved in authentication. But 43 and 44, all they say is that
14 in the present invention, the user terminal 50 itself, that will connect with the
15 service server 300 does not perform the authentication. That's exactly right.
16 It's not the user terminal 50 performing the authentication. In fact, if we
17 look back at figure 1 of Exhibit 1030, what we see is we see that there is a
18 authentication server over there, 200. That is what is actually performing
19 the authentication. So paragraphs 43 and 44 of *Lim* that just say the user
20 terminal is not performing the authentication, that doesn't mean that the user
21 terminal is not authenticated. It's just that the authentication processing is
22 happening elsewhere.

23 Dr. Meldal explains this in his declaration, and I think that should be
24 the end of it. You know, Patent Owner is just confused about what *Lim*
25 says.

1 In the end, *Lim*, as all the evidence confirms, *Lim* has authentication
2 both at the user terminal and at the mobile terminal. And because of that,
3 *Lim* is properly combined with *Kling*, and the modifications of *Kling* that I
4 discussed earlier obviate the claims.

5 So the final thing is claim construction. I did want to hit that with
6 the last of my time. So the claim construction issue is about the thereby
7 clause, whether that's limiting. Now, the Patent Owner has come in here and
8 said, well, the intent was to be limiting. But my question today, and the
9 question I struggle with, is what structure does that thereby clause add to
10 claim 41? What additional steps are necessary in the claim 26 process or
11 method?

12 Now, that thereby clause doesn't tell you. Patent Owner has come in
13 today and said, well, it requires isolation of information. And, you know, I
14 think we addressed this in our surreply at pages 4 to 5. What's happening
15 here and what seems to be happening here is that the Patent Owner seems to
16 be rewriting the thereby clause to mean forever protecting the second subset
17 of information so that it could never be accessed by someone with access to
18 the first device.

19 Now, Patent Owner had a number of opportunities to amend its
20 claims. It went through two rounds of amendments and it never made that
21 distinction. It never said, hey, you have to protect this information forever,
22 that the information can never be provided to the first device. So this
23 interpretation shouldn't be allowed. And in fact, this interpretation, as we
24 state -- as we've explained at the surreply pages 4 to 5, would actually
25 exclude the preferred embodiment, the poker embodiment, which is rarely, if
26 ever, correct. And that's because the poker -- even in the poker embodiment,

1 where the user has the second device as confirmation, the game server may
2 be unable to communicate with the second device when there is a network
3 connection disruption. And in that case, the game servers actually ask the
4 user at the first device if the user wants to continue with the game only on
5 the first device. So if malware was on that first device, of course, that would
6 be an instance where the malware would be able to get to the sensitive hole
7 card information.

8 So even under, you know, Patent Owner's attempt to say that this
9 claim could somehow mean that you can never get to the hole cards with the
10 first device, that's simply an embodiment that would exclude the preferred
11 embodiment. And according to the Federal Circuit, in *Vitronics v.*
12 *Conceptronic*, that's rarely ever correct.

13 So I think that's all I have to say on the claim construction issue.
14 Again, I want to reiterate that the patent at claim -- Exhibit 1001 at column
15 5, lines 56 to 63, when it shares the hole cards with the first device, it doesn't
16 say that they're no longer sensitive. That's attorney argument. It says there's
17 diminished value there. And Patent Owner's argued that, well, of course
18 they're no longer sensitive. But anyone who's played poker knows that if I
19 fold my hole cards, I don't have to show them to everybody. So there is
20 some sensitivity there, because I don't have to show my hand, I don't have to
21 show what I folded. And so when that gets sent back to the first device, as
22 part of keeping the hand history, I believe anyone who plays poker in this
23 room would know that those are still sensitive. So yeah, maybe they're
24 diminished value because the game is over, but it's still sensitive
25 information. So Patent Owner is just reading that part of the patent wrong.

1 And for those reasons, I think the claim construction issue is pretty
2 clear. Those are non-limiting examples -- or claim additions, and they
3 should be held to be non-limiting. And for all those reasons, I thank the
4 Board for this opportunity today. And I just ask that the Board would find
5 that these claims, these revised substitute claims, are not patentable for all
6 the reasons in our brief. Thank you.

7 JUDGE BARRETT: Thank you, Mr. Banner.

8 Mr. Benisek, you have 10 minutes.

9 MR. BENISEK: Thank you, Your Honors. Let me share my screen
10 again. Please let me know, I'm hoping to show the Board's preliminary
11 guidance order.

12 JUDGE BARRETT: Yes, we can see that.

13 MR. BENISEK: Great, page 17. What I highlighted is what I believe
14 was initially the Board's preliminary guidance on what the field endeavor
15 was, stated a little bit -- not directly, but I believe this is what the Board was
16 communicating, which was *Tsushima* -- or it says *Zha* and *Tsushima* are in
17 the same field of endeavor as the claimed invention because they also relate
18 to a system and method in which a user interacts with a first electronic
19 device and a second electronic device throughout the use of online
20 application. Understanding that was the Board's original finding. And then
21 there's a citation to Exhibit 1001, which is -- and the lines column 2, 29
22 through 31.

23 So I just want to comment first, sort of with all due respect to the
24 Board, we think that this finding was wrong. I think as a general matter, the
25 idea that a system and method in which the users interact with the first
26 electronic device and the second electronic device is not an actual field of

1 endeavor. All the Board has stated is it's taking a line from the specification,
2 but I don't think there's any evidence in the record that anyone, any POSITA
3 endeavors in this particular field what that is describing as the structure, a
4 portion of the structure used by the patent. And what I mean by that is when
5 you look at *Airbus*, when it found what's the field of endeavor? It said, oh,
6 fire prevention and suppression. In *Unwired*, cited by the Board, the field of
7 endeavor there was interface design.

8 And so, you know, we would submit that this isn't actually even a
9 proper field of endeavor. But I would also add that the citation to exhibit --
10 to the patent on these lines sort of omits that -- it's lines 29 through 31, but it
11 omits sort of a critical part of the description, which when we go there and
12 we look, here the Board cited column 2, lines 29 through 31. "Present
13 invention describes a system where the user's persistent use of a first device
14 and a second device throughout the use of an online application," and then it
15 stopped. But if you keep going, the rest of the sentence says, "to prevent the
16 compromise of transaction if malware infects your device." And I think that
17 is a proper statement of the field and endeavor. And I think you see that
18 repeated throughout. It's repeated at least -- it's obviously repeated in the
19 amended claims now, and it was at least repeated in claim 28 and it depends
20 in the initial filing.

21 So it's our position if following *Airbus*, you would look at this entire
22 statement, as well as all the other statements in the patent and the claims,
23 and you come to a much different field of endeavor than what the Board
24 originally came to.

25 And then just addressing the idea that claim 1 -- the Petitioner made
26 a statement about the law, which I don't believe is correct, which is, oh, just

1 look at claim 1, and then that's the field of endeavor for everything. The
2 Board is obligated to analyze each claim on a claim-by-claim basis for
3 invalidity and determine, you know, their independent validity. And the
4 field of endeavor and the scope of the claims are different. And we've
5 pointed that out with respect to claim 3 and the other claims in the patent.

6 JUDGE CHERRY: Where's your claim that -- we are supposed to
7 assess invalidity on a claim-by-claim basis, but I'm not sure that the Federal
8 Circuit has ever said we're supposed to do claim-by-claim for analogous art.
9 They usually talk about analogous art to the invention generally. Where --
10 do you have any citation for this claim-by-claim analogous art?

11 MR. BENISEK: Judge Cherry, I am just reacting to what Petitioner
12 said as a statement of the law. And so on the fly, I would just say that it's,
13 you know, our understanding of the law that you have to take each claim on
14 a claim-by-claim basis for validity, and that to the extent the claims vary in
15 their scope and what they cover, and at least original claim 3, you know, and
16 other depends, specify that there's sensitive information limitation, that those
17 should be considered on their own because they have a different scope than
18 claim 1. So I'll be happy to research and brief the issue post-hearing if the
19 panel would like.

20 JUDGE CHERRY: No, I'm not asking for more briefing. But, you
21 know, we'll take a look at it and, you know, if we need more briefing, we'll
22 ask for it. But at this point, I understand what your position is. Thank you.

23 MR. BENISEK: Okay. I guess turning to *Lim*, I mean, I think that the
24 Board is just going to have to read *Lim* for itself. We don't see -- I guess
25 there was -- I'll say this, there was a lot of attorney argument about what
26 paragraphs 28 and 29 say. And it was, what I would say, a lot of attorney

1 argument. When you read those paragraphs, I challenge the Board to find
2 anywhere in here where it says that the first device logs in with a username
3 and password, and then go and read paragraphs 43 and 44. So we just have
4 a fundamental difference there.

5 And then I will also add just another issue with *Lim* that we
6 addressed in our papers is that *Lim* describes all the authentication being
7 performed by the server service 200, which, as the claims require, it's the
8 server running the application that does the actual authentication. And so
9 that would be 300 if we were analyzing *Lim* consistent with the claims. But
10 what *Lim* discusses is 200 doing the authentication. And that is not the same
11 server as claimed in all the claims. So it's the second reason, it's a backup, I
12 would say, but equally valid why you wouldn't rely on *Lim* to modify a
13 claim.

14 And then finally, on the thereby clause, I guess there were just a
15 couple things I wanted to take issue with. The idea that this somehow, the
16 thereby clause, contradicts the preferred embodiment is actually incorrect.
17 The example Petitioner gave about the server being interrupted and then the
18 system dropping down to, you know, basically folding the game onto one
19 device is not claimed by Dr. Rubin. That is describing an unclaimed
20 embodiment, which would be if the user just decided I'm not going to play
21 poker using two devices, I'm just going to use one. When they do that,
22 they're clearly not practicing the patent. And so this idea that when the
23 game shares the -- when the system shares the hole cards with the first
24 device, in that situation it's discussing a completely unclaimed embodiment.
25 So it's not violating any preferred embodiment.

1 As I mentioned in our opening, there are many embodiments, the
2 banking, the healthcare, the brokerage that discuss only sending the second
3 subset of information and the sensitive information to the second device.
4 And there's no requirement that every embodiment be practiced by every
5 claim.

6 So with that, I think I've covered -- I tried not to go outside the
7 surrebuttal boundaries. And I thank the Board for consideration.

8 JUDGE BARRETT: All right, thank you. I see no questions from the
9 panel, so we are going off the record now. We're done with the arguments,
10 but please stay on the line for a second and I will ask the court reporter.

11 (Discussion off the record.)

12 JUDGE BARRETT: All right, thank you. Thank you, everyone.
13 Have a lovely day. And this case is submitted.

14 MR. BANNER: Thank you, Your Honors.

15 MR. BENISEK: Thank you, Your Honors.

16 (Whereupon, the proceedings at 3:09 p.m. were concluded.)

IPR2023-00693
Patent 9,064,376 B1

PETITIONER:

R. Beard
wbeard@sgbfirm.com
Rudolph Kim
rudylim@paulhastings.com
Naveen Modi
naveenmodi@paulhastings.com
Chetan Bansal
chetanbansal@paulhastings.com
Brian Banner
bbanner@sgbfirm.com

PATENT OWNER:

Robert McArthur
mcarthur@vbllaw.com