



UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

Kahoot! ASA & Kahoot Edu, Inc.

v.

Aviel D. Rubin

IPR2023-00693

U.S. Patent No. 9,064,376

Petitioner's Oral Argument – July 12, 2024

Asserted Grounds

Ground	Basis	Reference(s)	Challenged Claim(s)
Zha 1	§ 103	Zha + PGK*	26-29, 31, 34, 37, 39-41
Zha 2	§ 103	Zha + PGK + Tsushima	26-29, 31, 34, 37, 39-41
Zha 3	§ 103	Zha + PGK + Gumbula	30
Zha 4	§ 103	Zha + PGK + Tsushima + Gumbula	30
Zha 5	§ 103	Zha + PGK + Stafford	32
Zha 6	§ 103	Zha + PGK + Tsushima + Stafford	32
Zha 7	§ 103	Zha + PGK + Stafford + Gumbula	35
Zha 8	§ 103	Zha + PGK + Tsushima+ Stafford + Gumbula	35
Zha 9-16	§ 103	Zha Grounds 1-8 + Gui (lim. 26[c])	26-32, 34-35, 37, 39-41
Kling	§ 103	Kling + Lim + PGK	26-32, 34-35, 39-41
Takahashi 1	§ 103	Takahashi + PGK	26-35 and 37-41
Takahashi 2	§ 103	Takahashi + Tsushima + PGK	26-35 and 37-41
Takahashi 3-4	§ 103	Takahashi Grounds 1-2 + Gui (lim. 26[c])	26-35 and 37-41

*PGK = POSITA's General Knowledge

Proposed Agenda

- Overview of Revised Substitute Claims

- § 112 Deficiencies

- Claim Construction

- Zha Grounds 1-16

- Kling + Lim Ground

- Takahashi Grounds 1-4

Revised Substitute Claims

Revisions to Original Claims

- New limitations: claim 26[c] & 41[d]
 - “using application specific authentication information that is not authentication information specific to a device at both the first and second devices”
 - “wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device”

- New limitation: claim 28
 - “and the sensitive information is only shared with the second device”

Revisions to Original Claims

- New non-limiting language
 - “protecting information by” (claim 26[pre], 41[pre])
 - “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device” (claim 26[d] & 41[e])
- Claim 30
 - Depends from claim 28 (substitute for original claim 3) instead of claim 26 (substitute for original claim 1)
 - prior art teaching not disputed
- Claim 35
 - Duplicates “graphical identifier” / “graphical indicator” limitation from original claim 10
 - prior art teaching not disputed

§ 112 Deficiencies

§ 112 Deficiencies: Summary

- PO's burden to show substitute claims meet § 112 requirements
- Claims 26 and 41 lack written description support
 - “application specific authentication information that is not authentication information specific to a device at both the first and second devices” (claims 26[c] & 41[d])
- Claim 28 lacks written description support
 - “the sensitive information is only shared with the second device”
- Claims 32 and 35 are indefinite
 - “the information displayed on the respective devices”

**§ 112 Deficiencies: Claims 26 and 41 Lack
Written Description Support**

Substitute claims 26 and 41 require “not authentication information specific to a device” at both devices

Substitute claim 26[c]: “determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is **not authentication information specific to a device at both the first and second devices**, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device”

The '376 Patent only discloses application specific authentication information is not device specific only for the second device

- PO argues that the '995 Application “sufficiently describes the negative limitation of narrowing first device authentication by excluding non-device specific authentication information” and “disclose[s] using this precise embodiment...” Paper 30 (Reply), 2.
- But the '995 Application discusses the negative limitation only in the context of the second device:

[92] It should be noted that if an authentication token is used on the second device, then the user will be limited to using that specific device whenever using the application with the central server. If it is desired to be able to use different devices to serve as the second device in the application, then the authentication should be limited to the user entering authentication information, such as a password, into the second device, which can then be any device that contains the appropriate application software.

EX2005 ('995 Application)

The '376 Patent only discloses application specific authentication information is not device specific only for the second device

- PO's argument suggests that passwords are never device specific. Paper 30 (Reply), 2.
 - The '995 Application does not state that a password is always device independent.
 - PO contends that Kling's password for the second device is device specific. Paper 30 (Reply), 14; Ex-2009 ¶162.

**§ 112 Deficiencies: Claim 28 Lacks
Written Description Support**

Substitute claim 28 requires that sensitive information is only shared with the second device

“The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.”

Sensitive information in every embodiment of the '376 Patent is shared beyond the second device

- PO argues that sensitive “hole cards are only shared when the hand is over and the hole cards no longer constitute sensitive information.” Paper 30 (Reply), 2.
 - PO admits that the sensitive information is shared with the first device.
 - Claim 28 does not contemplate sharing at a later time or that the sensitive information may become not sensitive.

After the hand is completed, when any exposed cards, such as at a showdown, are sent to the player, the hidden hole cards can be sent to the first device, so that they can be stored in hand histories that are kept on the first device. More generally, after the information has diminished value, for example because the hand is completed, the information previously only visible on the second device can be sent to the first device. Beyond this particular application, many different

EX1001 ('376 Patent), 5:56–63

**§ 112 Deficiencies: Claims 32 and 35 are
Indefinite**

The scope of “the information displayed on the respective devices” in substitute claims 32 and 35 cannot be determined with reasonable certainty

“32. The method of claim 26, further comprising displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.”

“35. The method of claim 30, wherein, neither the first subset of information nor the second subset comprise a two factor authentication code, and,

further comprising displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.”

The scope of “the information displayed on the respective devices” in substitute claims 32 and 35 cannot be determined with reasonable certainty

- PO argues that the scope is “easily ascertainable by a POSITA.” Paper 30 (Reply), 3-4.
 - PO does not dispute the phrase lacks antecedent basis.
 - PO confirms the scope of this term cannot be determined by offering a myriad of different explanations of what the scope might be. Paper 30 (Reply), 3-4
 - “the online poker table on the first device and the hole cards on the second device”
 - “the hand displayed on the first device” and “the hole cards on the second device”
 - “hole cards [at the second device] and . . . community cards [at the first device]”
 - “the display of the application running simultaneously on the
 - two devices such as online poker game.”
 - PO’s expert offers yet another explanation of what the scope might be. EX2009 ¶83.
 - “the online application, such as online poker or banking”

Claim Construction

Terms requiring construction

- Two new phrases in the revised substitute claims require construction.
 - Preamble: “A method **for protecting information** by transmitting information to multiple electronic devices”
 - Limitations 26[d] (method) and 41[e] (apparatus): “**thereby protecting the second subset of the information . . . from potential malware on the first device**”
- PO argues these new phrases limit the claims. Paper 27 (Reply), 4-5.
- These phrases are non-limiting because they recite nothing more than a result of performing the claimed steps.

Phrases that state results of other limitations do not limit claims

“A ‘whereby’ clause that merely states the result of the limitations in the claim adds nothing to the patentability or substance of the claim.”

Texas Inst. Inc. v. U.S. Int’l Trade Comm’n, 988 F.2d 1165, 1172 (Fed. Cir. 1993)
(citing *Israel v. Cresswell*, 166 F.2d 153, 156 (1948)).

Undisputed: Protecting information occurs as a result of performing the other claimed limitations

- Substitute claim 26[d]: “if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.” See *also* Claim 41[e] (same).

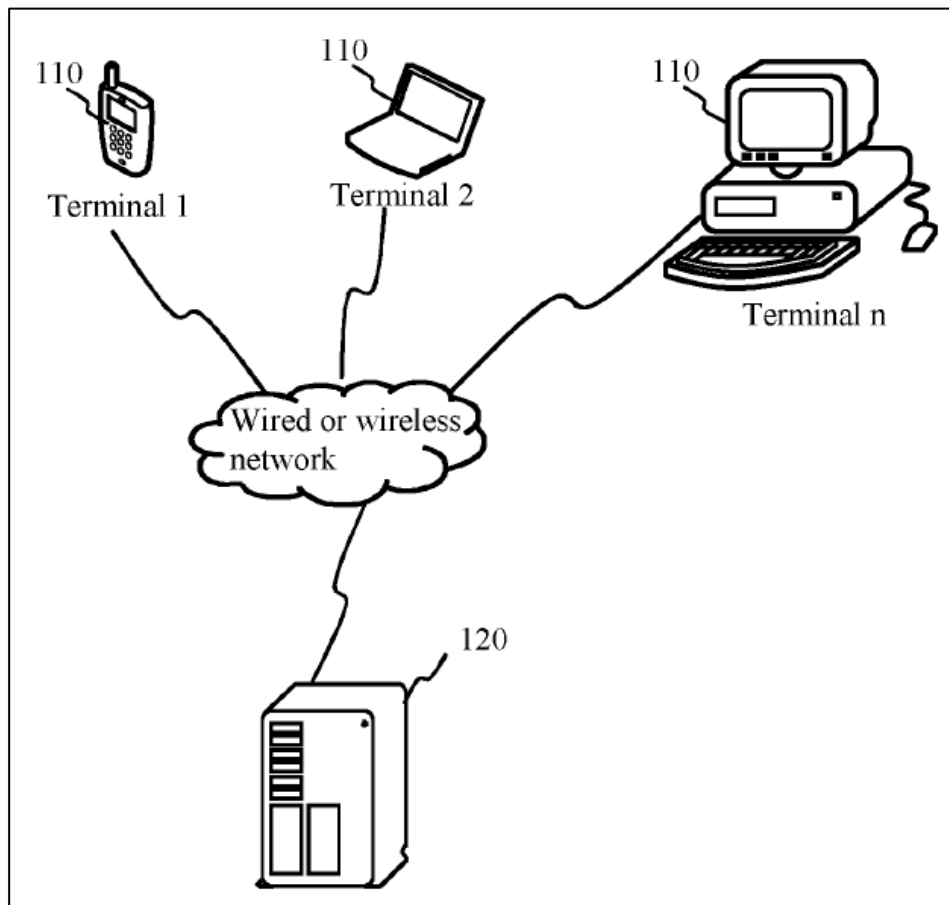
84. In my opinion, the “thereby” clause of claim 26[d] and 41[e] adds to the patentability of the claims. The claims require that a second subset of information is sent by the application to only the second device. This isolation of information provides protection to the second subset of information because it is not exposed to malware that has potentially compromised the first device.

EX2009 (3rd Traynor Decl.), ¶ 84

Zha Grounds 1-16

Zha overview: Zha discloses a microblog application that a user can log in and access simultaneously with two different terminals

more terminals simultaneously. At least two terminals 110, which run an application program with the same account simultaneously, and a server 120 may be included in the implementation environment, as is shown in FIG. 1.



For example, in a case the user logs in to microblog in the cellphone, the laptop computer and the desktop computer simultaneously, and sets the cellphone as the multifunction terminal, the user may simultaneously send application requests for the three terminals, i.e., the cellphone, the laptop computer and the desktop computer, as illustrated in FIG. 5B for details. For the laptop computer and the desktop com-

EX1004 (Zha), 18:11-17

EX1004 (Zha), 4:21–24, Fig. 1

Undisputed: Zha Grounds 1-8 disclose all original claim limitations

G. Summary

Accordingly, Petitioner has shown there is a reasonable likelihood that it would prevail in proving that challenged claim 1 would have been obvious over Zha, when viewed in the context of POSITA's knowledge. Pet. 2 (Ground 1).

H. Other Claims and Other Grounds

Petitioner also contends that claims 2–4, 9, 13, 14, 16, and 23–25 are unpatentable under 35 U.S.C. § 103 over Zha and POSITA's knowledge. Pet. 2 (Ground 1). Petitioner further contends that claims 1–4, 9, 13, 14, 16, and 23–25 are unpatentable under 35 U.S.C. § 103 over other prior art references and POSITA's knowledge. *Id.* (Grounds 2–8). As indicated above, Patent Owner does not present any arguments or evidence related to Petitioner's patentability challenges. *See* Prelim. Resp. 1–9. We have reviewed Petitioner's evidence and arguments regarding those claims and grounds and on this record, we find that Petitioner has shown a reasonable likelihood of prevailing on those claims and grounds as well.

Paper 10 (Institution Decision), 20

Pet. 2. Patent Owner does not present any arguments or evidence related to Petitioner's patentability challenges. *See* Prelim. Resp. 1–9.

Paper 10 (Institution Decision), 11

Original Claims: Zha discloses a login process to determine whether a single user has logged into the same microblog application at two terminals

In Zha's method, the server receives a request from the two terminals for "running the same application program with the same account simultaneously." Ex. 1004, 5:17–18. Zha also discloses a login process to determine whether a single user has logged into the same microblog application at two terminals. *See id.* at 18:41–49. Petitioner provides evidence of POSITA's general knowledge that a login process can be used to ensure that an electrical device is being directly operated by and in possession of a particular user. *See* Ex. 1002 ¶¶ 76–80; Ex. 1007 ¶¶ 109–110; Ex. 1010 ¶¶ 41, 57, Fig. 7A.

Paper 10 (Institution Decision), 18

Original Claims: Zha discloses the first and second subsets of information are transmitted “if and only if” a user has logged into the microblog application with two devices

In Zha’s method, if (and only if) the server receives a request from the two terminals for running the same application program (e.g., microblog application) with the same account simultaneously, the first subset of information (e.g., homepage interface data) is sent to the first terminal (e.g., the user’s laptop computer) and the second subset of information (e.g., private message data) is sent to the second terminal (e.g., the user’s cellphone). See Ex. 1004, 5:17–27, 18:66–19:19, Fig. 2B, 8; Ex. 1002 ¶¶ 82–84. The second subset of information (e.g., the private message data) includes information not transmitted to the first terminal (e.g., the user’s laptop computer). See Ex. 1004, 10:48–50.

Thus, on the present record and for the purposes of institution, we determine that Petitioner has demonstrated sufficiently that Zha discloses or suggests the features recited in claim 1’s step (iv).

Paper 10 (Institution Decision), 19 (undisputed)

Zha Grounds 1-16: Disputes

Zha Grounds 1-16: Disputes

- PO makes four (4) arguments:
 - First Argument: Zha fails to disclose authenticating a user on two devices as claimed in 26[c] (i.e., using different application specific authentication information that is not device specific). Paper 30 (Reply), 6-10.
 - Board's Preliminary Guidance correctly concludes Zha + POSITA's knowledge teaches authentication (log in) from two devices using application specific authentication information (passwords). Paper 21 (Preliminary Guidance), 19.
 - Using different passwords for Zha's different devices is obvious based on POSITA's knowledge and Zha + Gui.

Zha Grounds 1-16: Disputes

- PO makes four (4) arguments:
 - Second Argument: Zha fails to disclose “protecting information” as recited in the thereby clause of 26[d]. Paper 30 (Reply), 10-11.
 - “Protecting information” phrases are non-limiting.
 - Even if these phrases are limiting, Zha discloses protecting private messages from malware on the first device (e.g., desktop computer) by sending private messages “only to the cellphone...”

Zha Grounds 1-16: Disputes

- PO makes four (4) arguments:
 - Third Argument: Zha fails to disclose “the sensitive information is only shared with the second device” as recited in Claim 28. Paper 30 (Reply), 11-12.
 - Zha expressly discloses an embodiment where private messages are sent “only to the cellphone...”
 - PO’s teaching away argument here (and elsewhere) does not satisfy the legal test for teaching away which requires a reference to “criticize, discredit, or otherwise discourage investigation into the invention claimed.” *Galderma Laboratories, L.P. v. Tolmar, Inc.*, 737 F.3d 731, 739 (Fed. Cir. 2013) (quotations omitted).
 - PO’s interpretation of this limitation, i.e., where sensitive information cannot be shared beyond the second device, would exclude every embodiment in the ’376 Patent.

Zha Grounds 1-16: Disputes

- PO makes four (4) arguments:
 - Fourth Argument: Zha is not analogous art. Paper 30 (Reply), 18; Paper 22 (RMTA), 24-25.
 - Board's Preliminary Guidance is correct. Paper 21 (Preliminary Guidance), 24-25.
 - PO improperly relies on the alleged point of novelty to define the field of endeavor
 - PO improperly relies on the alleged problem addressed to define the field of endeavor
 - PO's addition of non-limiting phrases for "protecting information" should not affect the field of endeavor

Zha Grounds 1-16: Claims 26[c] / 41[d]

PO's First Argument: Zha does not teach different application specific authentication information for different devices

26[c] / 41[d]: Zha's login uses "application specific authentication information"

Kling teaches this amended limitation. We find Patent Owner's argument that Zha does not teach "application specific authentication information" unpersuasive because Zha disclosing a user logging in to the account of a microblog application program through two or more terminals appears to correspond to providing information for authentication that is specific to the microblog application, consistent with our preliminary construction of the term "application specific authentication information" discussed above. *See also* Opp. 18–19. We also find that Petitioner's rationale for the

Paper 21 (Preliminary Guidance), 19

26[c] / 41[d]: Zha's "application specific authentication information" (passwords) are "not authentication information specific to a device"

- Both experts agree passwords were well known authentication information used for accessing online applications

196. I evaluate the patentability of the revised substitute claims based on Patent Owner's apparent reliance on the disclosure of using two different specific passwords to authenticate the first and second devices. In view of this assumption, it was well known by 2014 that password authentication could be used for logging into an application such as Zha's microblog (e.g., Facebook login). In fact, a 2006

EX1029 (3rd Meldal Decl.), ¶196

Abstract. Passwords are currently the dominant authentication mechanism in computing systems. However, users are unwilling or unable to retain passwords

EX1024-001 (Traynor Article, 2006)

26[c] / 41[d]: Zha's "application specific authentication information" (passwords) are "not authentication information specific to a device"

- According to PO, passwords for accessing online applications are application specific and not device specific

4 A. I don't think I understand. If I
5 have a username and password, that is specific to
6 each application. So the username and password I
7 use for my bank, that's application specific. My
8 username and password that I use for social media
9 application, that's specific to that application.

EX1026-018 (Traynor Dep. Tr.), 72:4-9

be obvious to a person of ordinary skill in the art. The passwords are not device
specific because Zha does not disclose that the logins from the two terminals are
specific to those two terminals.

EX1029 (3rd Meldal Decl.), ¶196

26[c] / 41[d]: Zha's "application specific authentication information" (passwords) are "not authentication information specific to a device"

- According to PO, passwords for accessing online applications are application specific and not device specific

the second device.” Ex. 2005, ¶90, Ex. 2009, ¶73-75. Further, the specification teaches the advantages and disadvantages of limiting the authentication process to non-device specific authentication information, which was a known concept to a POSITA and applied to all device attempting to access web applications. Ex. 2005, ¶92, Ex. 2009, ¶73-75. *Applying Navartix Pharms. Corp., the '376 Patent*

Paper 30 (PO Reply), 2

26[c] / 41[d]: Obvious based on POSITA's knowledge to use different passwords on different devices to access online applications

- Zha Grounds 1-8: Gui is evidence of POSITA's general knowledge that different devices can use different passwords to access the same account.

These and other problems are overcome by the present invention which provides systems and methods for the association of multiple sets of credentials to a single user account. An authentication system is provided that allows a user to be authenticated using different credentials. Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

EX1031 (Gui), 2:20-29

26[c] / 41[d]: Obvious based on POSITA's knowledge to use different passwords on different devices to access online applications

One problem that often presents itself in these situations is related to the access devices that are used to access a computer based service. More specifically, the problem is related to the credentials that a user must supply in order to sign or log in to a computer based service. Credentials have to be entered into the access device when a user is signing in to a computer based service. Different devices have different form factors as well as different data input capabilities and while providing credentials on one device may be a relatively straightforward task, providing the same credentials on another device may prove to be a burdensome task.

For example, assume that a user has an email account and that the user is able to access the email account using the following credential:

Username: Joe@emailservice.com

Password: myPAssword.

When the user attempts to access their email account from a desktop computer, the credential can be quickly and easily entered using the keyboard because the user is able to quickly and easily select and enter upper/lower case letters as well as special characters. In contrast, when the user attempts to access their email account from their cellular phone, the task of logging in by entering this credential becomes significantly more difficult. The user is typically required to “triple-tap” on the numbers in order to select each letter in both the username and the password, navigate complex menu systems to select upper/lower case letters, and find symbols such as the “@” character. If the user

EX1031 (Gui), 1:39-2:3

26[c] / 41[d]: Obvious based on POSITA's knowledge to use different passwords on different devices to access online applications

241. In other words, at the time of the '376 Patent (in fact, earlier), *Gui* teaches that some passwords are more difficult to enter on a mobile phone compared to entering the same password on a computer that has a full keyboard. *Gui* suggests an easy solution to this problem for any service that allows login to the same account by both mobile phones and desktop/laptop computers. *Gui*'s solution is to allow the user to have multiple passwords for logging into the same account/service. I note

EX1029 (3rd Meldal Decl.), ¶241

- Lipetz and Kling also provide evidence of POSITA's knowledge
 - See Ex1029 (3rd Meldal Decl.) ¶200-204

26[c] / 41[d]: Obvious based on Zha + Gui to use different passwords on different devices to access online applications

- Zha Grounds 9-16 (Zha + Gui): Gui's multiple different passwords combined with Zha's microblog application

26[c] / 41[d]: Obvious based on POSITA's knowledge or (Zha + Gui) to use different passwords on different devices to access online applications

- Gui provides motivation to modify Zha's microblog application

209. Finally, *Gui* provides additional motivation to use multiple passwords in a system such as *Zha* that utilizes different hardware devices—human interface accessibility. Specifically, *Gui* explains:

210. As evidenced by *Gui*'s disclosure, a POSITA's knowledge includes the understanding of the benefit of allowing multiple different passwords in a system like *Zha* that provides for easy human interface access via desktop computer and mobile phone. Consequently, a POSITA would find it obvious based on this knowledge to allow the user to use different passwords on the different devices when logging into *Zha*'s microblog.

EX1029 (3rd Meldal Decl.), ¶209-210 (citing EX1031, 1:39-2:3)

Zha Grounds 1-16: Claims 26[d] / 41[e]

PO's Second Argument: Zha fails to disclose “protecting information” as recited in the thereby clause of 26[d]

26[d] / 41[e]: Zha teaches protecting information as recited in preamble and thereby clause

- “Protecting information” clauses are not limiting
- Nevertheless, Zha teaches protecting information
 - Private messages are sent “only to the cellphone”

by microblog to the desktop computer, the server may send a private message only to the cellphone without sending the private message to the laptop computer or the desktop computer when needing to sending the private message to a terminal logging in with the account. Since the private

EX1004 (Zha), 19:3–13

- Dr. Traynor admits this isolation protects the information

84. In my opinion, the “thereby” clause of claim 26[d] and 41[e] adds to the patentability of the claims. The claims require that a second subset of information is sent by the application to only the second device. This isolation of information provides protection to the second subset of information because it is not exposed to malware that has potentially compromised the first device.

EX2009 (3rd Traynor Decl.), ¶ 84

Zha Grounds 1-16: Claim 28

PO's Third Argument: Zha fails to disclose sensitive information shared only with second device

28: Zha's server only shares the sensitive private message with the cellphone terminal

“28. The method of claim 26, wherein the first subset of the information comprises **non-sensitive information**; and the second subset of the information comprises **sensitive information** and the sensitive information is **only shared with the second device**.”

sion for accessing the functional interface for display. For example, in a case the server assigns the access permission for accessing the private message interface to the cellphone, assigns an access permission for accessing a homepage interface to the laptop computer and assigns access permissions for accessing the other functional interfaces provided by microblog to the desktop computer, the server may send a private message only to the cellphone without sending the private message to the laptop computer or the desktop computer when needing to sending the private message to a terminal logging in with the account. Since the private

EX1004 (Zha), 19:3–13

Zha Grounds 1-16: Non-Analogous Art

PO's Fourth Argument: Zha is not analogous art

PO's non-analogous art argument should be rejected

- PO relies on an incorrect legal test to argue Zha and Takahashi (and Tsushima) are non-analogous art
- Petitioner's response is the same for all references

Board's preliminary guidance is correct: Zha and Takahashi are from the same field of endeavor as the substitute claims

Google Inc., 841 F.3d 995, 1001 (Fed. Cir. 2016). Here, Zha and Tsushima are in the same field of endeavor as the claimed invention because they also relate to a system or method in which a user interacts with “a first [electronic] device and a second [electronic] device throughout the use of an online application.” Ex. 1001, 2:29–31. Based on

Paper 21 (Preliminary Guidance), 17–18

Takahashi is in the same field of endeavor as the claimed invention because it also relates to a system or method in which a user interacts with “a first [electronic] device and a second [electronic] device throughout the use of an online application.” Ex. 1001, 2:29–31. Based on the current

Paper 21 (Preliminary Guidance), 24–25

Art is analogous when in the same field of endeavor – even if it addresses a different problem

“Two separate tests define the scope of analogous prior art: ‘(1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.’”

Airbus S.A.S. v. Firepass Corp., 941 F.3d 1374, 1379 (Fed. Cir. 2019) (citing *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004)).

PO improperly relies on the alleged point of novelty of the substitute claims

“The field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field.”

Unwired Planet, LLC v. Google Inc., 841 F.3d 995, 1001 (Fed. Cir. 2016).

PO improperly argues that Zha and Takahashi are not analogous because they do not address the same problem as the '376 Patent

“[W]e are also persuaded by Petitioner’s argument that Patent Owner is wrong to assert that the prior art must address the same problem as the '376 patent. See Opp. [Paper 20] 24 (citing *Ex parte Talkowski*, Appeal No. 2012-00290 (PTAB May 24, 2013) (informative)).”

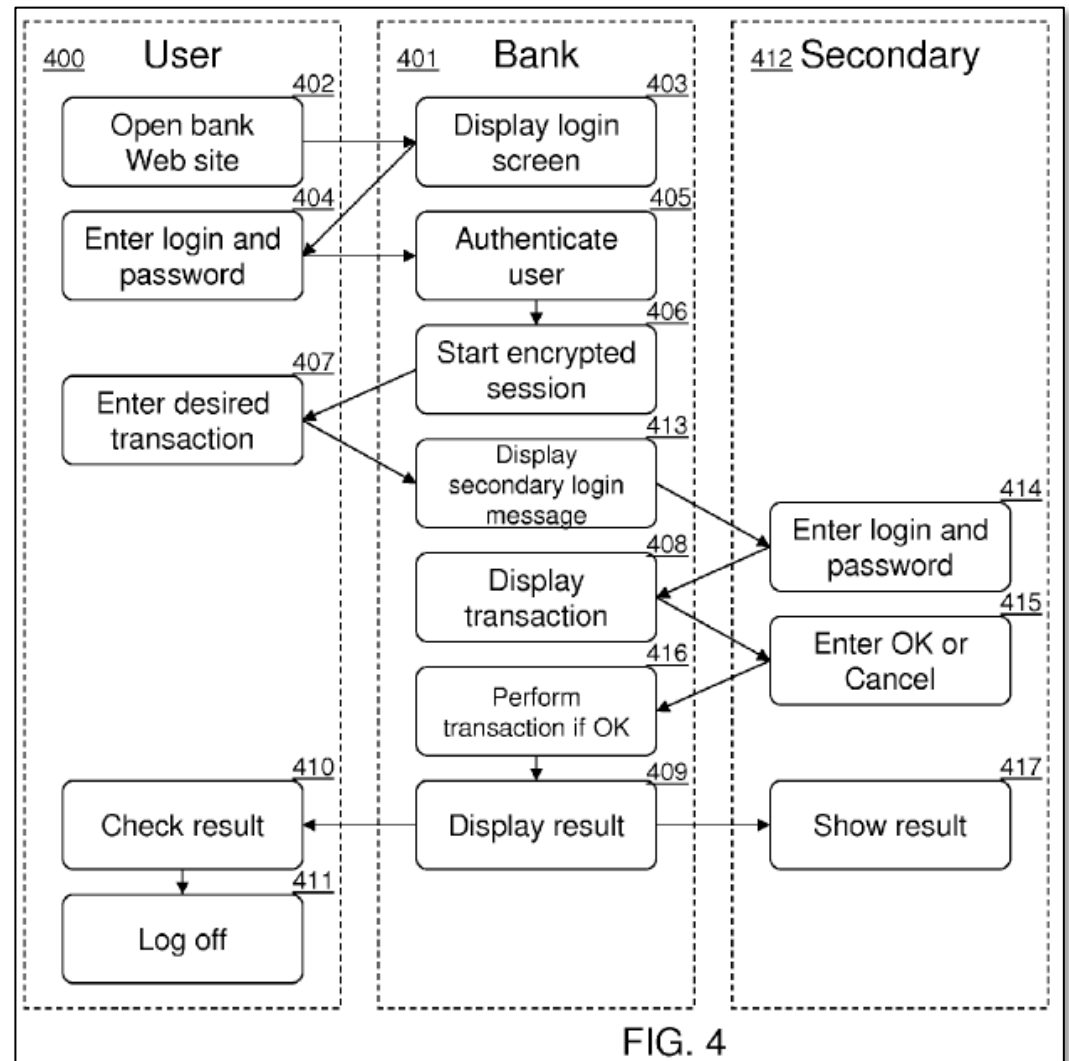
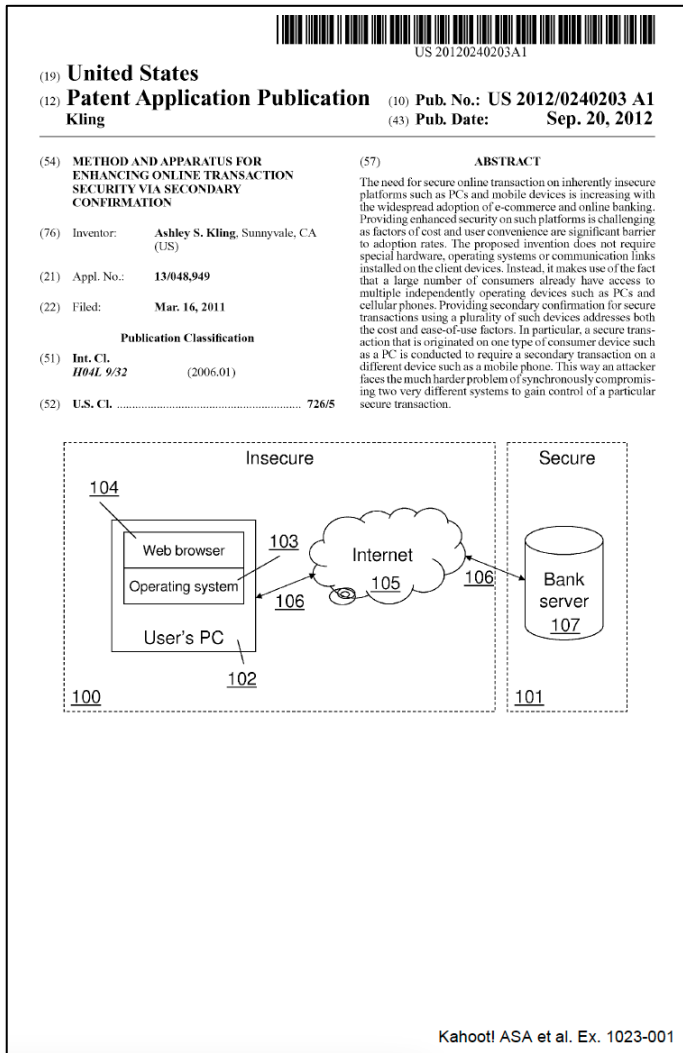
Paper 21 (Preliminary Guidance), 18 (emphasis added)

PO's non-limiting amendments: “protecting information”

- Non-limiting amendments in IPR should not affect field of invention
 - Claim 26 and 41 Preamble: “A method **for protecting information** by transmitting information to multiple electronic devices”
 - Limitations 26[d] and 41[e]: “**thereby protecting the second subset of the information . . . from potential malware on the first device**”
- Allowing this would encourage mischief by patent holders faced with invalidating prior art

Kling + Lim Ground

Undisputed: Kling discloses limitations 26[p], 26[a], and 26[b]



EX1023 (Kling), Fig. 4

Kling + Lim Ground: Disputes

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - First Argument: Kling fails to disclose claim 26[c] because Kling's mobile phone login is device specific and does not log into the banking application. Paper 30 (Reply), 14-15.
 - PO's argument ignores the Board's Preliminary Guidance and Kling's express disclosure that the mobile phone logs into the banking application.

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - Second Argument: Kling + Lim fails to disclose claim 26[c] because Lim only discloses authenticating with one device (the mobile phone). Paper 30 (Reply), 14-15.
 - PO ignores Lim's express teaching that both the user terminal and the mobile phone authenticate.

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - Third Argument: Kling + Lim fails to disclose claim 26[c] because Lim's authentication information is device specific. Paper 30 (Reply), 14-15.
 - PO ignores Lim's express teaching that the authentication information is not device specific (e.g., passwords, biometric information, etc.).

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - Fourth Argument: Kling + Lim fails to disclose claim 26[c] because Lim teaches away from a combination with Kling. Paper 30 (Reply), 14-15.
 - PO's teaching away argument does not satisfy the legal test for teaching away which requires a reference to "criticize, discredit, or otherwise discourage investigation into the invention claimed." *Galderma Laboratories, L.P. v. Tolmar, Inc.*, 737 F.3d 731, 739 (Fed. Cir. 2013) (quotations omitted).

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - Fifth Argument: Kling fails to disclose the “if and only if” limitation of 26[d] / 41[e] (i.e., waiting to send the first subset of information until after both devices are authenticated). Paper 30 (Reply), 12-14.
 - Petitioner’s evidence shows a POSITA would modify Kling based on Lim’s teaching in one of two ways, and PO fails to address the first modification, i.e., “mov[ing] Kling’s mobile device login steps ... earlier in time to coincide with the PC login steps.”
 - This evidence is unrebutted.
 - For Petitioner’s second modification, PO incorrectly argues that only the mobile phone in Lim is authenticated where Lim expressly discloses both the mobile phone and the desktop are authenticated.

Kling + Lim Grounds: Disputes

- PO makes six (6) arguments:
 - Sixth Argument: Kling fails to disclose claim 28's sensitive information is only shared with the second device. Paper 30 (Reply), 15.
 - PO does not address the evidence on which Petitioner relies, i.e., evidence that shows sensitive information (web transaction confirmation information) is only sent to the second device (mobile phone).

Kling + Lim Ground: Claims 26[c] / 41[d]

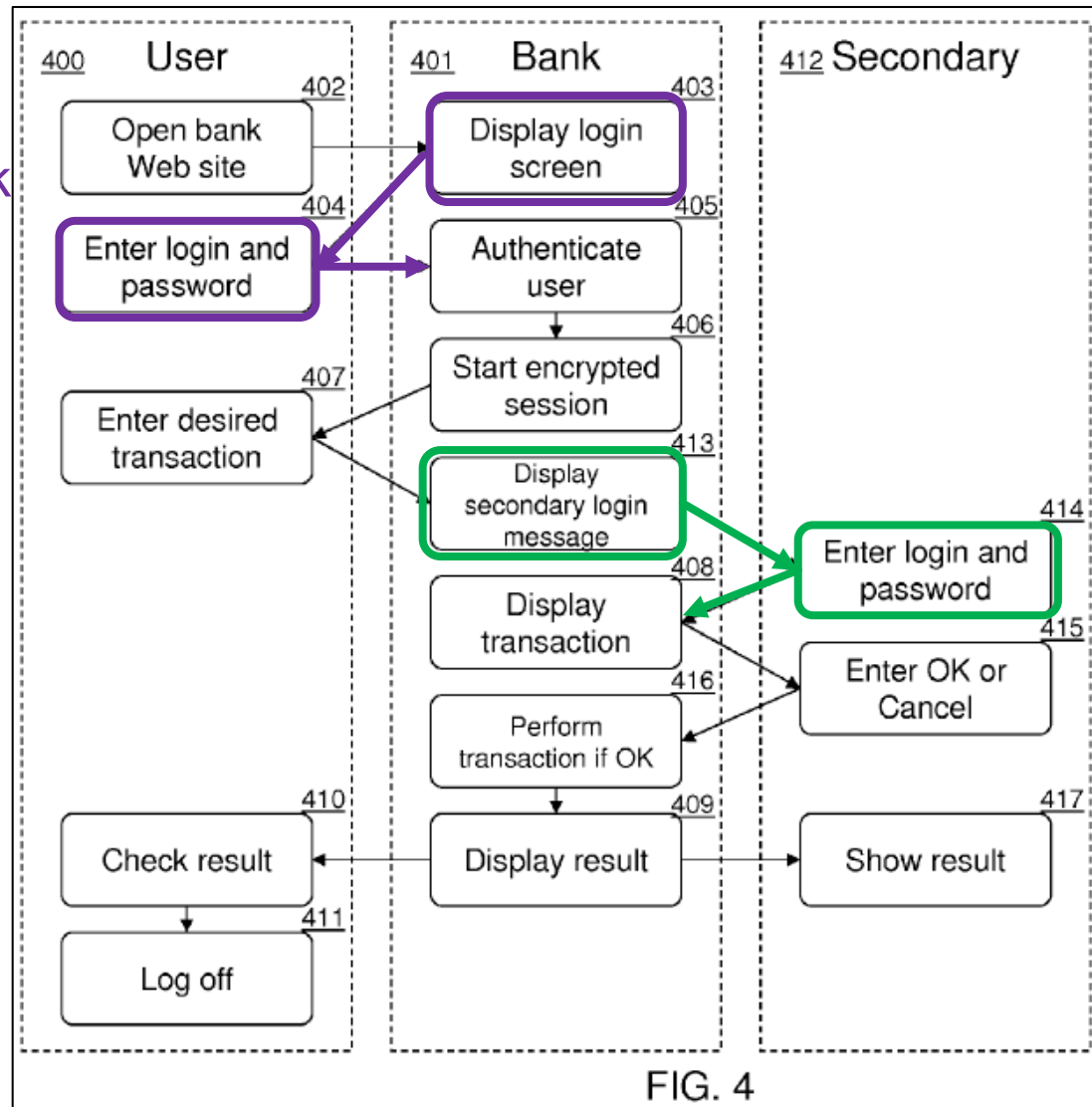
PO's First Argument: Kling's mobile phone login is device specific and does not log into the banking application

26[c] / 41[d]: Kling's mobile phone logs into the banking application

Kling teaches requiring the user to “approve a specific secure transaction on a mobile device in addition to the original transaction performed on a PC.” Ex. 1023 ¶ 7. Figure 4 shows that a user enters a password (at step 404) for a bank Web site on a first device 400 (e.g., PC) to initiate a desired transaction. *See id.* ¶ 17; *see also id.* ¶ 14. Figure 4 also shows that the user is further prompted to enter a password (at step 414) on a second device 412 (e.g., mobile device) as secondary authentication. *See id.* ¶ 17. Kling teaches that “[t]ypically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.” *Id.* ¶ 18. Petitioner’s reading of Kling appears to be consistent with our preliminary construction of “application specific authentication information” because the user’s password in Kling appears to correspond to information for authentication (e.g., a different password for secondary authentication) that is specific to an application (e.g., a bank Web site).

Paper 21 (Preliminary Guidance), 15

26[c] / 41[d]: Kling's mobile phone logs into the banking application



EX1023 (Kling), Fig. 4

log into bank server with second device

“Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.”

EX1023 (Kling), [0018]

Kling + Lim Ground: Claims 26[c] / 41[d]

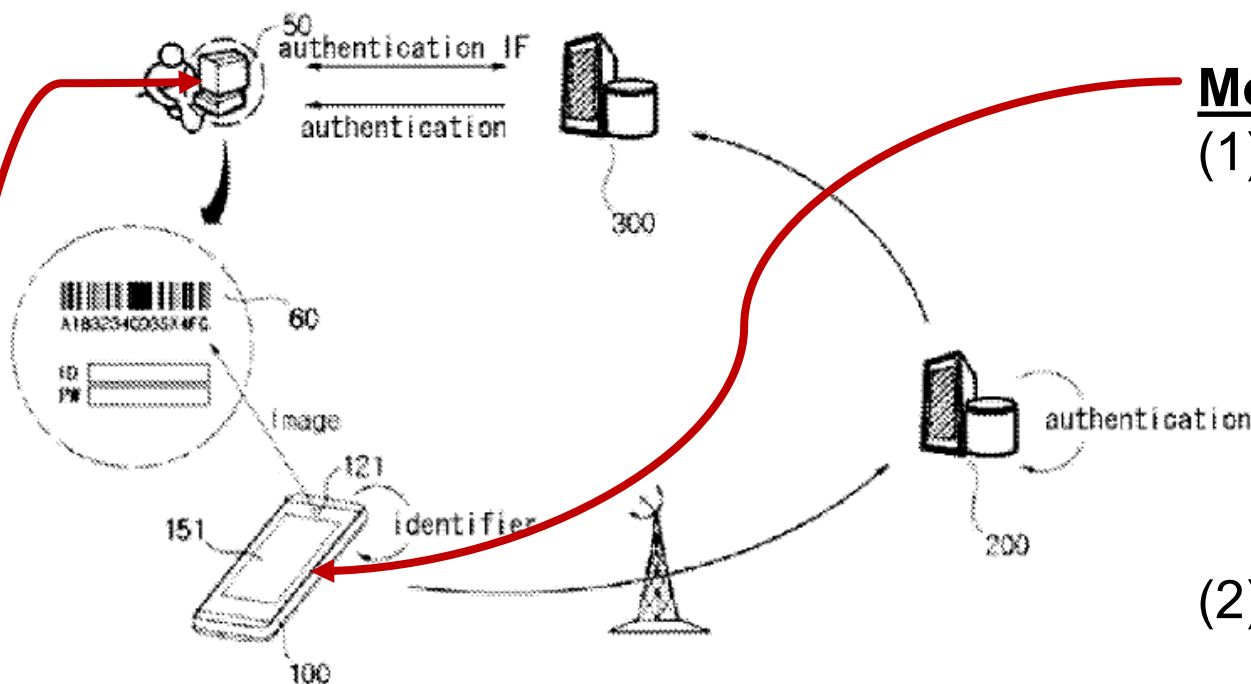
**PO's Second Argument: Lim only discloses authenticating
with one device (the mobile phone)**

26[c] / 41[d]: Lim discloses allowing a transaction “if and only if” the user is authenticated.

[0077] Once the success of the authentication has been notified by the authentication information processing module 250, the service server 300 determines that the user terminal 50 has been successful in the authentication, allows normal access, and provides a variety of services that can be utilized by a login user. If the service server 300 is the server of a financial institution, such as a bank, the service server 300 allows the user terminal 50 to do an account transfer, search an account, use a loan service, pay a utility bill, and use a variety of services that are provided by the financial institution such as a bank.

EX1030 (Lim), [0077]

26[c] / 41[d]: Lim authenticates a user on two devices using different authentication information



EX1030 (Lim), Figure 1

User Terminal 50

The user enters an ID and PW via the authentication interface displayed on the user terminal 50

EX1030 (Lim), [0029]

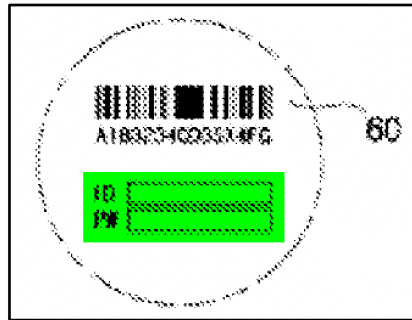
Mobile Terminal 100

- (1) User captures identifier 60 from the screen of user terminal 50 by reading the identifier (bar code) with the camera of mobile terminal 100.
- (2) Mobile terminal 100 sends identifier information to authentication system 200.
- (3) User enters non-device specific authentication information to authenticate mobile terminal 100

EX1030 (Lim), [0033–42]

26[c] / 41[d]: Lim discloses accessing an online application using different authentication information for two different devices

Authentication information for user terminal 50



[0028] Referring to FIG. 1, in an authentication method according to the present invention, when the user terminal 50 connects with the service server 300 and performs authentication, for example, performs login, the service server 300 provides an authentication interface including an identifier to the user terminal 50.

[0029] The authentication interface shown in FIG. 1 includes an input box for receiving an identifier/password and an identifier 60.

EX1030 (Lim), [0028–29] & Fig. 1

Authentication information for mobile terminal 100

[0038] The authentication system 200 generates the identifier information from the identifier that the service server 300 has provided to the user terminal 50, and compares the identifier information with identifier information provided by the mobile terminal 100, thereby determining the validity of the identifier information. Thereafter, if it is determined that the identifier information is valid, the authentication system 200 requests authentication information from the mobile terminal 100, and the mobile terminal 100 provides the authentication information to the authentication system 200, thereby performing a final authentication process. Here, the authentication information may be any one of the following:

[0039] an identifier/password,

[0040] an authentication number that was agreed with a user,

[0041] biometric information such as iris information, a fingerprint, or a voice, and

EX1030 (Lim), [0038–41]

26[c] / 41[d]: Lim discloses accessing an online application using different authentication information for two different devices

➤ User terminal 50 authentication info

- Identifier/password

➤ Mobile terminal 100 authentication info

- Identifier/password
- Authentication number
- Biometric information

Lim discloses different authentication information

User terminal 50	Mobile terminal 100	Different?
Identifier/password	Identifier/password	☒ PGK
Identifier/password	Authentication number	☒
Identifier/password	Biometric information	☒

Kling + Lim Ground: Claims 26[c] / 41[d]

**PO's Third Argument: Lim's authentication information is
device specific**

26[c] / 41[d]: Lim's authentication information is not device specific

➤ User terminal 50 authentication info

- Identifier/password

➤ Mobile terminal 100 authentication info

- Identifier/password
- Authentication number
- Biometric information

Passwords used to access web applications are not device specific

the second device.” Ex. 2005, ¶90, Ex. 2009, ¶73-75. Further, the specification teaches the advantages and disadvantages of limiting the authentication process to non-device specific authentication information, which was a known concept to a POSITA and applied to all device attempting to access web applications. Ex. 2005, ¶92, Ex. 2009, ¶73-75. Applying *Navartix Pharms. Corp.*, the '376 Patent

Paper 30 (PO Reply), 2

26[c] / 41[d]: Lim's authentication information is not device specific

➤ User terminal 50 authentication info

- Identifier/password

➤ Mobile terminal 100 authentication info

- Identifier/password
- Authentication number
- Biometric information

Lim discloses a web application

website of a financial institution such as a bank. Furthermore, the service server may be any of a variety of types of websites that provide information to users, personal homepages, a variety of websites that require login, and specific websites that ask subscribers for their information when they subscribe to the websites.

EX1030 (Lim), [0024]

26[c] / 41[d]: Lim's authentication information is not device specific

➤ User terminal 50 authentication info

- Identifier/password

➤ Mobile terminal 100 authentication info

- Identifier/password
- Authentication number
- Biometric information

Lim's authentication number and biometric information are user specific

[0040] an authentication number that was agreed with a user,

[0041] biometric information such as iris information, a fingerprint, or a voice, and

EX1030 (Lim), [0040]–[0041]

Kling + Lim Ground: Claims 26[c] / 41[d]

PO's Fourth Argument: Lim teaches away from a combination with Kling

26[c] / 41[d]: Lim's use of device specific authentication information does not teach away from the claimed invention

- PO's teaching away argument does not satisfy the legal test for teaching away which requires a reference to "criticize, discredit, or otherwise discourage investigation into the invention claimed." *Galderma Laboratories, L.P. v. Tolmar, Inc.*, 737 F.3d 731, 739 (Fed. Cir. 2013) (quotations omitted).

Kling + Lim Ground: Claims 26[d] / 41[e]

PO's Fifth Argument: transmitting distinct subsets of information to the PC and mobile device if and only if both devices are accessible by the bank server

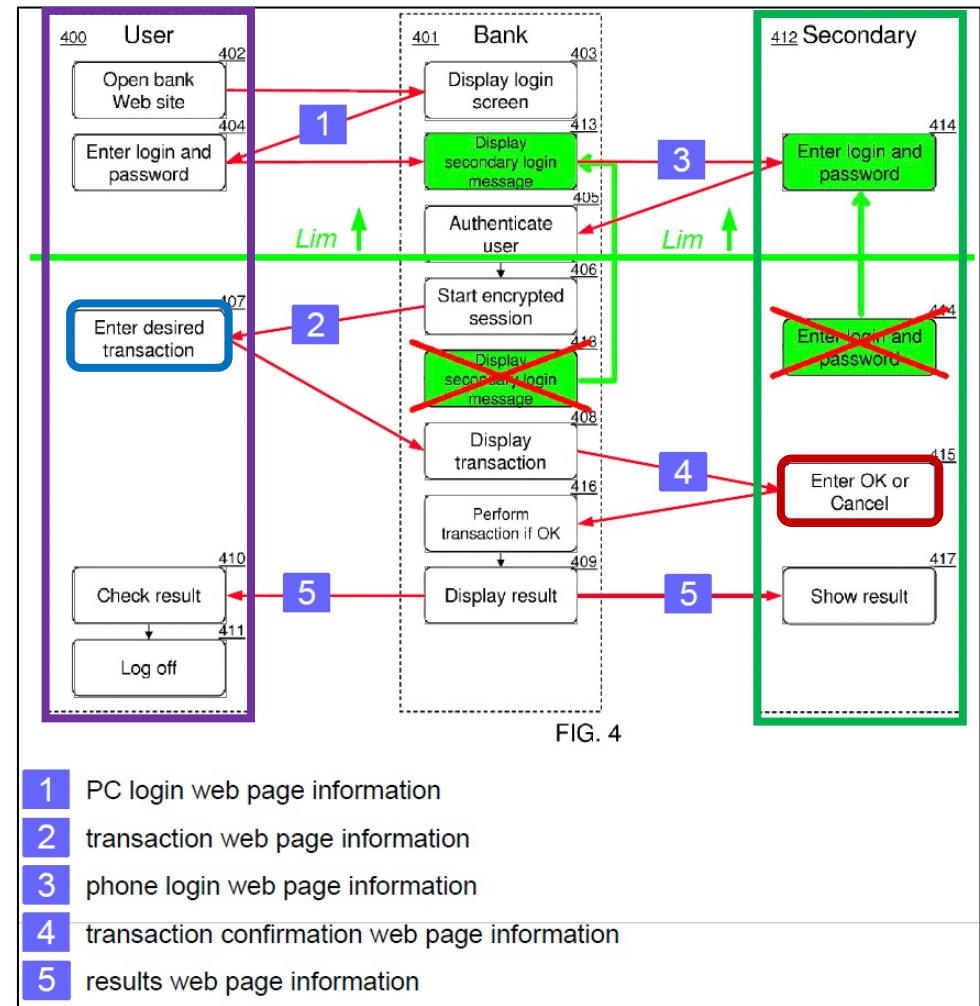
26[c] / 41[d]: Lim discloses allowing a transaction “if and only if” the user is authenticated.

[0077] Once the success of the authentication has been notified by the authentication information processing module 250, the service server 300 determines that the user terminal 50 has been successful in the authentication, allows normal access, and provides a variety of services that can be utilized by a login user. If the service server 300 is the server of a financial institution, such as a bank, the service server 300 allows the user terminal 50 to do an account transfer, search an account, use a loan service, pay a utility bill, and use a variety of services that are provided by the financial institution such as a bank.

EX1030 (Lim), [0077]

26[d] / 41[e]: Kling + Lim teaches transmitting distinct subsets of information to the PC and mobile device if and only if both devices are accessible by the bank server

“if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the **first subset of the information** to the **first device** from the server; and transmitting the **second subset of the information** to the **second device** from the server”

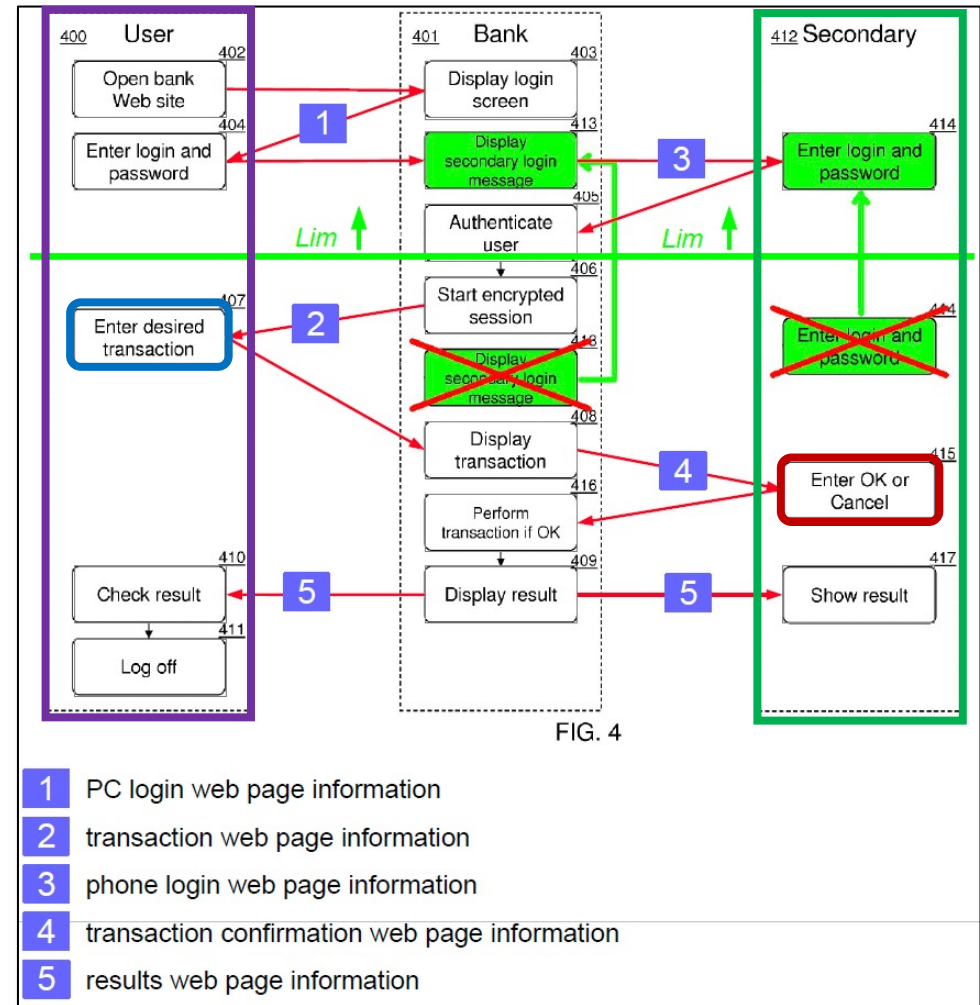


EX1023 (Kling), Fig. 4 (modified)

26[d] / 41[e]: Kling + Lim teaches transmitting distinct subsets of information to the PC and mobile device if and only if both devices are accessible by the bank server

- Petitioner's evidence shows a POSITA would modify Kling based on Lim's teaching in one of two ways, and PO fails to address the first modification, i.e., "mov[ing] Kling's mobile device login steps ... earlier in time to coincide with the PC login steps." EX1029 (3rd Meldal Decl.) ¶134.

- This evidence is un rebutted.



EX1023 (Kling), Fig. 4 (modified)

26[d] / 41[e]: Kling + Lim teaches transmitting distinct subsets of information to the PC and mobile device if and only if both devices are accessible by the bank server

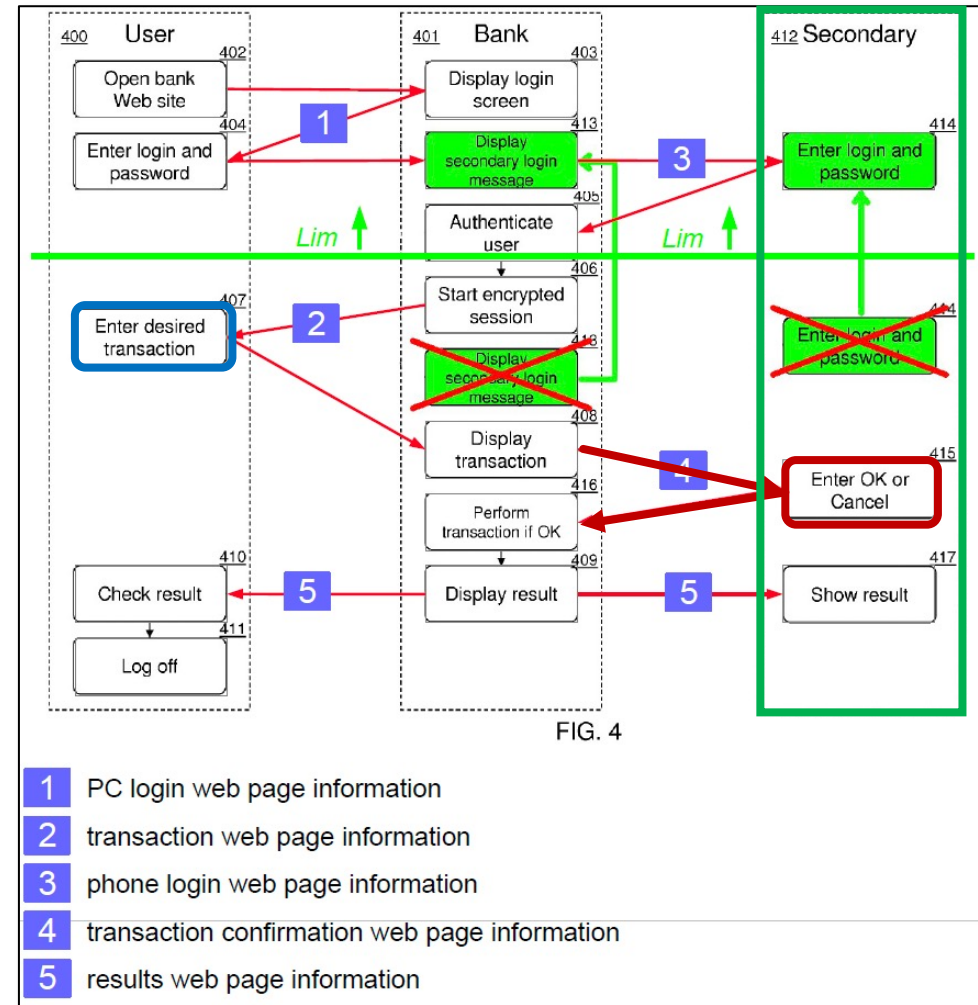
- For Petitioner's second modification, PO incorrectly argues that only the mobile phone in Lim is authenticated where Lim expressly discloses both the mobile phone and the desktop are authenticated.

Kling + Lim Ground: Claim 28

PO's Sixth Argument: Kling fails to disclose sensitive information is only shared with the second device

Claim 28: Kling discloses sensitive information is sent only to the second device

“The method of claim 26, wherein the first subset of the information comprises **non-sensitive information**; and the second subset of the information comprises **sensitive information** and the sensitive information is **only shared with the second device**.”

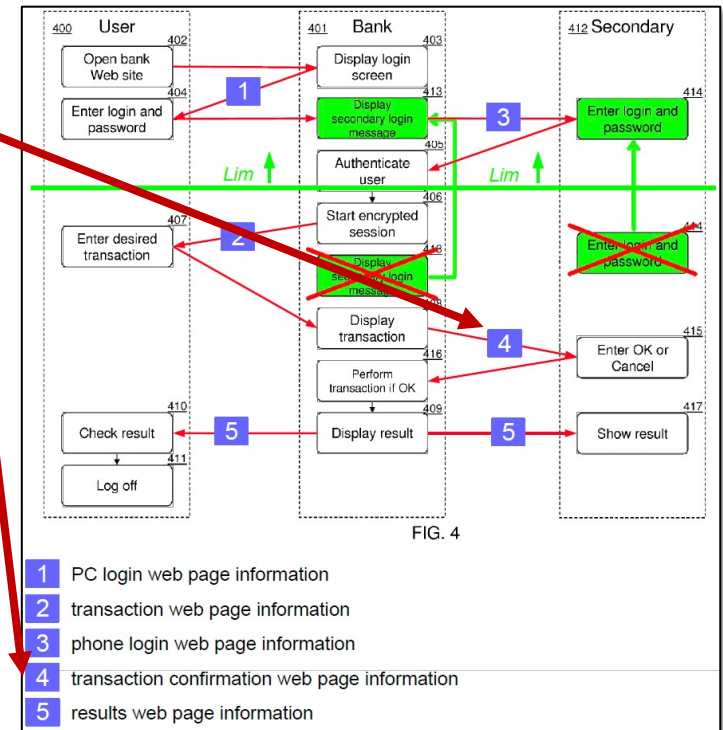


EX1023 (Kling), Fig. 4

Claim 28: Kling discloses sensitive information is sent only to the second device

145. Further, the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to “display transaction” 408 so the user may “enter OK or Cancel” 415 corresponds to the second subset of information, which comprises “sensitive information,” as claimed. The invitation enabling the approval of a transfer of funds and providing the means to do so, such as transaction identifiers or cookies, (the “OK” response) is clearly sensitive because it provides the ability to finally perform a critical transaction such as transferring money to an external account.

EX1029 (3rd Meldal Decl.) ¶145



Kling + Lim Ground

Claims 27, 29–35, 39, 40

Kling + Lim teaches the additional limitations of substitute claims 27, 29–35, 39, 40

- PO does not separately argue the dependent claim limitations

C. *Kling* Does Not Disclose Substitute Claims 27, 29, 31, 32, 34, 35, 39, 40, 41

For the reasons stated in Patent Owners April 5, 2024 Revised Motion to Amend (Paper 22), *Kling* and its combinations fail to disclose Substitute Claims 27, 29, 31, 32, 34, 35, 39, 40 and 41.

Paper 30 (PO Reply ISO RMTA), 15

- Note: Claim 30 is not mentioned but depends from claim 28, which is addressed in previous slides

Takahashi Grounds

Undisputed: The Takahashi grounds disclose all limitations of the unamended challenged claims

H. Other Claims and Other Grounds

Petitioner also contends that claims 2–4, 9, 13, 14, 16, and 23–25 are unpatentable under 35 U.S.C. § 103 over Zha and POSITA’s knowledge. Pet. 2 (Ground 1). Petitioner further contends that claims 1–4, 9, 13, 14, 16, and 23–25 are unpatentable under 35 U.S.C. § 103 over other prior art references and POSITA’s knowledge. *Id.* (Grounds 2–8). As indicated above, Patent Owner does not present any arguments or evidence related to Petitioner’s patentability challenges. *See* Prelim. Resp. 1–9. We have reviewed Petitioner’s evidence and arguments regarding those claims and grounds and on this record, we find that Petitioner has shown a reasonable likelihood of prevailing on those claims and grounds as well.

Paper 10 (Institution Decision), 20

Pet. 2. Patent Owner does not present any arguments or evidence related to Petitioner’s patentability challenges. *See* Prelim. Resp. 1–9.

Paper 10 (Institution Decision), 11

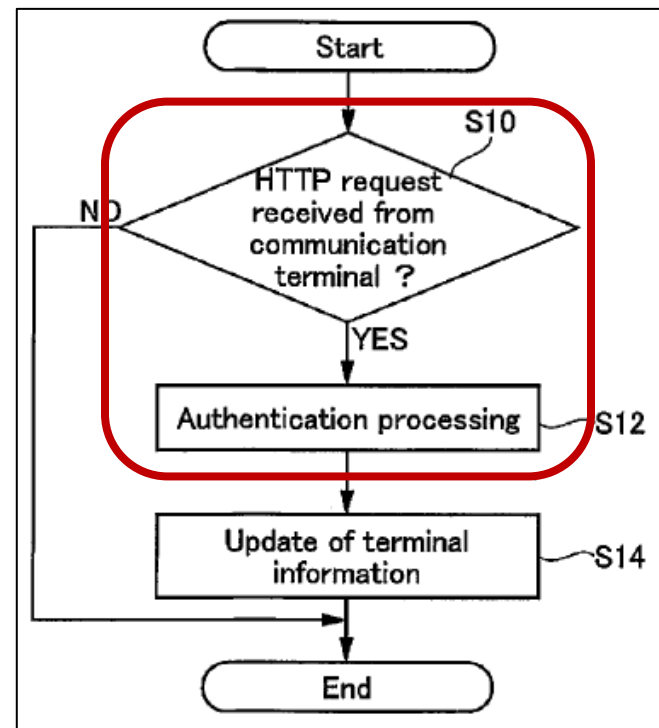
Takahashi Grounds: 26[c] / 41[d]

**different application specific authentication information for
different devices**

26[c] / 41[d]: Takahashi discloses authentication as part of the log-in process

logs in to the game server 20. In this case, in response to an operational input by the user to communication terminal (mobile terminal 10 or PC 12), a HTTP request (access request) is transmitted from the mobile terminal 10 or the PC 12 to the game server 20. The HTTP request transmitted from the mobile terminal 10 includes identification information. The HTTP request transmitted from the PC 12 includes a user ID and a password that have been inputted to the PC 12. After receiving the HTTP request (Step S10: YES), the game server 20 performs authentication processing (Step S12). In the authentication processing, the identification information, or the user ID and the password, which are included in the HTTP request, are identified first. The game server 20 then collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is

EX1007 (Takahashi), [0110]



EX1007 (Takahashi), Fig. 11

performs authentication processing (Step S12).” While the wording (which was originally in Japanese) may suggest two separate processes, a POSITA would understand the overall description of the process of Figure 11 to be normal password authentication where a username and password (and other “identification information”) are provided as part of the HTTP request in step S10 in Figure 11. Ex. 1007, [0110], Figure 11). The server then checks that information against the user data in the user database and grants access if there is a match. Ex. 1007, [0110].

EX1029 (3rd Meldal Decl.), ¶ 272

26[c] / 41[d]: Takahashi does not rely on device-specific authentication information

tions of the acceptor 52 are realized as described below. After receiving a HTTP request as access request from the mobile terminal 10 or the PC 12 of the user, the CPU 21 of the game server 20 identifies identification information, or user ID and a password, based on user agent character strings included in the HTTP request. The CPU 21 collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is one from any of the registered users, the CPU 21 accepts the access request.

EX1007 (Takahashi), [0095]

275. A POSITA reading this passage understands that *Takahashi's* use of the word “or” means the user may login with (1) user ID and password or (2) identification information. A POSITA also understands that the user ID and password is not specific to a device, which corresponds to revised amended claim 26[c]. Whether *Takahashi* also teaches using “a serial number of the mobile

EX1029 (3rd Meldal Decl.)

26[c] / 41[d]: Takahashi does not rely on device-specific authentication information

tions of the acceptor 52 are realized as described below. After receiving a HTTP request as access request from the mobile terminal 10 or the PC 12 of the user, the CPU 21 of the game server 20 identifies identification information, or user ID and a password, based on user agent character strings included in the HTTP request. The CPU 21 collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is one from any of the registered users, the CPU 21 accepts the access request.

EX1007 (Takahashi), [0095]

275. A POSITA reading this passage understands that *Takahashi's* use of the word "or" means the user may login with (1) user ID and password or (2) identification information. A POSITA also understands that the user ID and password is not specific to a device, which corresponds to revised amended claim 26[c]. Whether *Takahashi* also teaches using "a serial number of the mobile

EX1029 (3rd Meldal Decl.)

26[c] / 41[d]: Takahashi + Gui teaches different passwords for different devices

- Takahashi Grounds 1-2: Gui is evidence of POSITA's general knowledge

These and other problems are overcome by the present invention which provides systems and methods for the association of multiple sets of credentials to a single user account. An authentication system is provided that allows a user to be authenticated using different credentials. Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

EX1031 (Gui.), 2:20-29

- Takahashi Grounds 3-4: Gui's multiple different passwords combined with Takahashi's game application

26[c] / 41[d]: Takahashi + Gui teaches different passwords for different devices

- Gui provides motivation to modify Takahashi's application

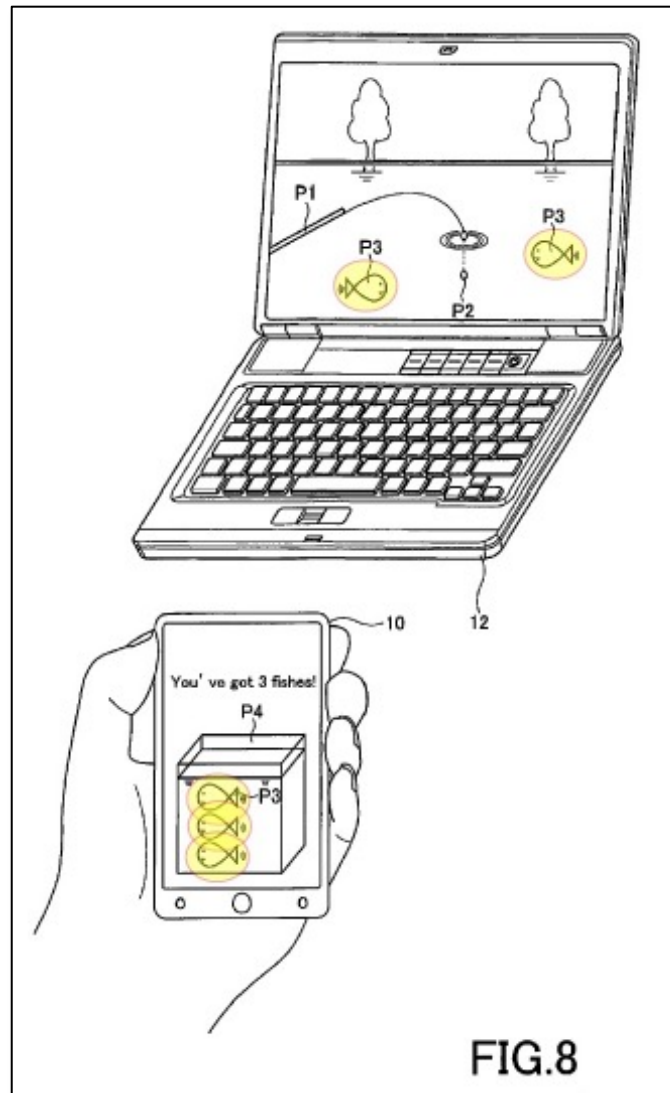
283. It is my opinion a POSITA would be motivated to combine *Gui* with the other prior art (Grounds 7-8) for the same reasons I provide above in Section X.A, which I incorporate herein by reference. Consequently, it is my opinion that substitute claims 26-35 and 37-41 are unpatentable based on the *Takahashi* Grounds as modified by *Gui*'s disclosure of using multiple/different passwords with different devices.

EX1029 (3rd Meldal Decl.), ¶282-285

Takahashi Grounds: 27

same information in first and second subsets of information

27: Takahashi's game server sends the same data to both terminals



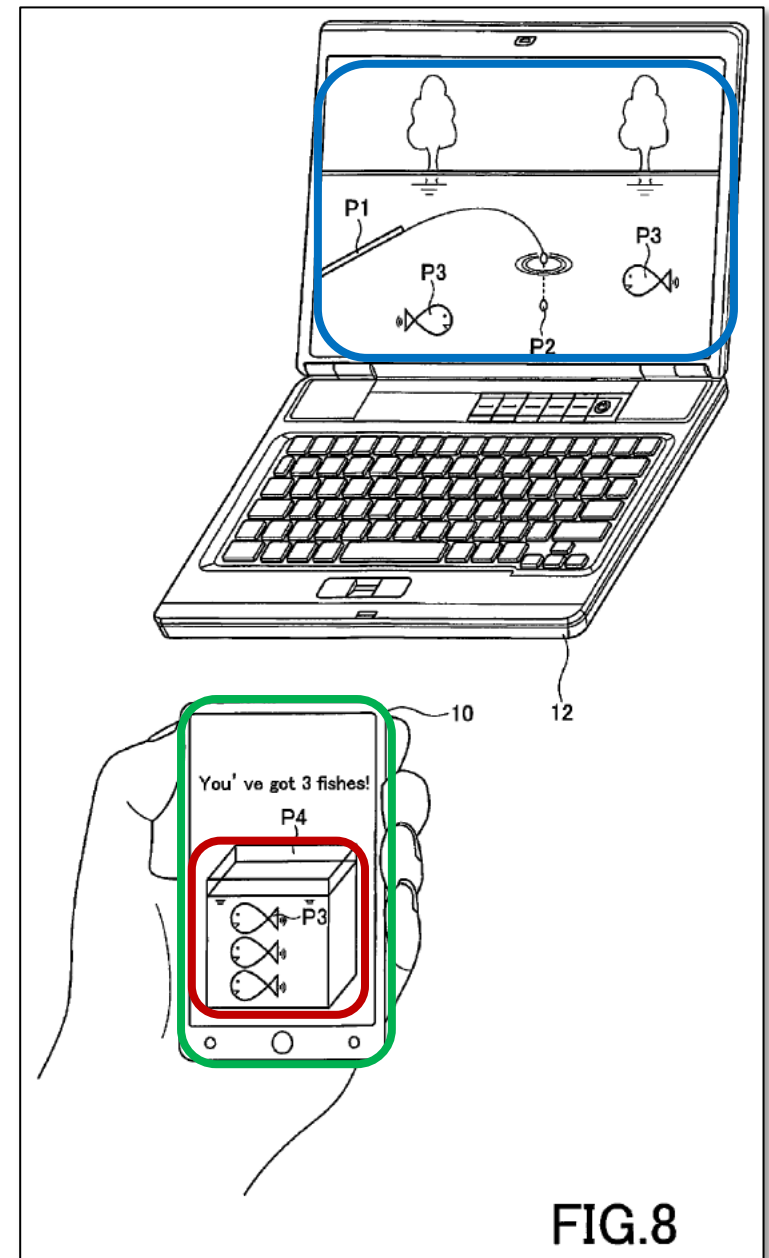
EX1007 (Takahashi), Fig. 8

Takahashi Grounds: 28

sensitive information shared only with second device

28: Takahashi shares individual game score only with mobile device

“The method of claim 26, wherein the first subset of the information comprises **non-sensitive information**; and the second subset of the information comprises **sensitive information** and the sensitive information is **only shared with the second device**.”



EX1007 (Takahashi), Fig. 8

28: Takahashi's individual game score is “sensitive information”

Ex. 1007, Figure 8 (annotated). Further, the game results (e.g., the user's score shown on the mobile device in Figure 8) is “sensitive” in the context of *Takahashi's* second embodiment where “the users may compete for a number of fish objects that are taken in a period of time in the game.” Ex. 1007, [0122]. In this scenario (multi-player games such as the fishing game or other known multi-player games), knowing another player's score could provide a player with an unfair advantage.

EX1002 (1st Meldal Decl.) ¶262