

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA & KAHOOT EDU, INC.,
Petitioner

v.

AVIEL D. RUBIN,
Patent Owner.

Case No. IPR2023-00693

Patent No. 9,064,376

**PATENT OWNER'S NON-CONTINGENT
MOTION TO AMEND U.S. PATENT NO. 9,064,376**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	PRELIMINARY GUIDANCE FROM THE BOARD.....	2
III.	THE PROCEDURAL REQUIREMENTS OF 37 C.F.R. . § 42.121 ARE SATISFIED.....	2
	A. SUBSTITUTE CLAIMS ARE PROVIDED IN A CLAIMS LISTING.....	2
	B. THE NUMBER OF SUBSTITUTE CLAIMS IS REASONABLE.....	2
	C. THE AMENDMENTS ARE RESPONSIVE TO THE GROUNDS AT ISSUE.....	3
	D. THE AMENDMENTS ARE NON-BROADENING.....	3
	E. THE AMENDMENTS HAVE WRITTEN DESCRIPTION SUPPORT.....	3
IV.	PERSON OF ORDINARY SKILL IN THE ART (POSITA).....	8
V.	CLAIM CONSTRUCTION.....	8
VI.	THE PROPOSED SUBSTITUTION CLAIMS ARE PATENTABLE OVER THE INSTITUTED GROUNDS AND ART.....	10
	A. ZHA DOES NOT TEACH OR SUGGEST THE LIMITATIONS PROPOSED FOR THE SUBSTITUTE CLAIMS.....	11
	B. TSUSHIMA DOES NOT TEACH OR SUGGEST THE LIMITATIONS PROPOSED FOR THE SUBSTITUTE CLAIMS.....	14
	C. TAKAHASHI DOES NOT TEACH OR SUGGEST THE LIMITATION PROPOSED FOR THE SUBSTITUTE CLAIMS.....	15

D. ZHA, TSUSHIMA AND TAKAHASHI ARE NOT “ANALOGOUS” PRIOR ART.....	19
E. THERE IS NO MOTIVATION TO COMBINE.....	23
VII. CONCLUSTION.....	25

TABLE OF AUTHORITIES

CASES

<i>Airbus S.A.S. v. Firepass Corp.</i> , 941 F.3d 1374 (Fed. Cir. 2019).....	20
<i>Aqua Prods., Inc. v. Matal</i> , 872 F. 3d 1290 (Fed. Cir. 2017).....	11
<i>CUPP Computing AS v. Trend Micro Inc.</i> , 53 F. 4th 1376 (Fed. Cir. 2022).....	8
<i>Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC</i> , 57 F. 4th 1001 (Fed. Cir. 2023).....	8
<i>Intuitive Surgical, Inc. v. Ethicon LLC</i> , IPR2018-00933, Paper 31 (PTAB Dec. 3, 2019).....	1
<i>Lectrosonics, Inc. v. Zaxcom, Inc.</i> , IPR2018-01129, Paper 15 (PTAB Feb. 25, 2019).....	2, 11
<i>Phillips v. AWH Corp.</i> , 415 F. 3d 1303 (Fed. Cir. 2005).....	9

STATUTES

35 U.S.C. § 316(d)(2).....	1
37 C.F.R. § 1.121(c)(2).....	2
37 C.F.R. § 42.100(b).....	9

OTHER

MPEP § 2141.01(A).....	19, 20
------------------------	--------

LIST OF EXHIBITS

Exhibit No.	Description
2004	Declaration of Patrick Traynor, Ph.D. in support of Patent Owner's Non-Contingent Motion to Amend U.S. Patent No. 9,064,376
2005	U.S. Patent Application No. 14/444,995
2006	U.S. Provisional Application No. 62/008,561
2007	A Guide through 7 Microblogging Websites, published at https://www.linkedin.com/pulse/guide-through-7-microblogging-websites-realytviews/

I. INTRODUCTION

Patent Owner Dr. Aviel D. Rubin (“Rubin” or “Patent Owner”) respectfully submits this Non-Contingent Motion to Amend (“Motion”) to request amendment of challenged claims 1-5, 9-10, 12-17, and 23-25 of U.S. Patent No. 9,064,376 (“the ’376 Patent”) in order to provide further clarification of the invention set forth therein. Pursuant to 35 U.S.C. § 316(d)(2) and Notice, 84 Fed. Reg. at 9497, Patent Owner submits this Motion proposing new substitute claims 26-41 (the “Substitute Claims” set forth in Appendix A) for original claims 1-5, 9-10, 12-17, and 23-25 (the “Challenged Claims”) of the ’376 Patent.

Because Patent Owner is not concurrently filing a Response and this motion is non-contingent, the Board need not address the patentability of the originally challenged claims 1-5, 9-10, 12-17, and 23-25. *See, e.g., Intuitive Surgical, Inc. v. Ethicon LLC*, IPR2018-00933, Paper 31 at 3 n.5 (PTAB Dec. 3, 2019) (“Because we grant the Motion to Amend, which is a non-contingent motion, ... we need not address the patentability of [the challenged claims].”). Substitute Claims 26, and 41 retain features of original independent claims 1 and 25, and the substitutions add narrowing features. The proposed Substitute Claims are responsive to the grounds of unpatentability at issue in this proceeding and are supported by the application as originally filed.

II. PRELIMINARY GUIDANCE FROM THE BOARD.

Patent Owner requests preliminary guidance from the Board on this Motion to Amend pursuant to the Motion to Amend (MTA) Pilot Program, initiated on March 15, 2019. 84 Fed. Reg. 9497; Scheduling Order, Paper 11 at 4-6.

III. THE PROCEDURAL REQUIREMENTS OF 37 C.F.R. § 42.121 ARE SATISFIED.

A. SUBSTITUTE CLAIMS ARE PROVIDED IN A CLAIMS LISTING.

The claim listing is attached as Appendix A. The claim listing cancels original claims 1-5, 9-10, 12-17, and 23-25 and includes Substitute Claims 26-41. The Substitute Claims include annotations pursuant to 37 C.F.R. § 1.121(c)(2). Moreover, the remaining statutory and regulatory requirements for a motion to amend are met.

B. THE NUMBER OF SUBSTITUTE CLAIMS IS REASONABLE.

Pursuant to 37 C.F.R. § 42.121(a)(3), the number of Substitute Claims is reasonable. “There is a rebuttable presumption that a reasonable number of substitute claims per challenged claim is one (1) substitute claim.”

Lectrosonics, Inc. v. Zaxcom, Inc., IPR2018-01129, Paper 15 at 4 (PTAB Feb. 25, 2019). Patent Owner proposes 16 non-contingent Substitute Claims (claims 26-41), each of which corresponds to the 16 Challenged Claims (original claims 1-5, 9-10, 12-17, and 23-25). The number of substitute claims presented is presumptively reasonable based on the one-to-one relationship. *Id.*

C. THE AMENDMENTS ARE RESPONSIVE TO THE GROUNDS AT ISSUE.

The proposed Substitute Claims are responsive to the Grounds at issue in this proceeding because they further distinguish the claims from the art of record. For instance, the Substitute Claims provide clarity by adding limitations relating to the disclosure of the '376 Patent for using authentication information for logging into the application at the first device that is different from the authentication information that is used to log into the application at the second device. For this reason, and as further explained below, the Substitute Claims are patentable over the instituted Grounds.

D. THE AMENDMENTS ARE NON-BROADENING.

The Substitute Claims do not seek to enlarge the scope of the original claims. Dependent Substitute Claims 27-40 all depend from Substitute claim 26, and thus are narrowed by the narrowing amendment to Substitute claim 26. Substitute dependent claims 27-40 also include all of their original limitations, in addition to Substitute claims 30 and 35 containing new additional narrowing limitations. Accordingly, all of the proposed amendments are narrowing.

E. THE AMENDMENTS HAVE WRITTEN DESCRIPTION SUPPORT.

Each of the proposed Substitute Claims 26-41 have written description support in the U.S. Patent Application No. 14/444,995 ("the '995 App.") (now U.S. Patent No. 9,064,376)(Exhibit 2005). As shown in the table below, each limitation of the

Substitute Claims is disclosed in the specification and/or figures of the '995 App.

Claim	Claim Element of Substitute Claim	'995 App. (Ex. 2005)
[26 Pre]	A method for transmitting information to multiple electronic devices, the method comprising:	¶2; ¶18-19; ¶23-25
[26a]	electronically storing a set of information at a server;	Fig. 5-6; ¶25; ¶38; ¶39; ¶89-90
[26b]	identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	¶23-28; ¶38
[26c]	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 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.	Fig. 10; ¶26; ¶33; ¶75; ¶83; ¶89; ¶90; ¶92
[26d]	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.	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; ¶23-29 ¶33-34; ¶58; ¶65; ¶78; ¶82;
[27]	The method of claim 26, further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.	¶24; ¶38-39; ¶45; ¶48;

[28a]	The method of claim <u>26</u> , wherein the first subset of the information comprises non-sensitive information; and	¶30-32;
[28b]	the second subset of the information comprises sensitive information.	¶30-32; ¶35; ¶57; ¶78; ¶82;
[29]	The method of claim <u>26</u> , wherein the information received at the second device is more sensitive than the information received at the first device.	¶24; ¶30-32; ¶35; ¶57; ¶78;
[30]	The method of claim <u>28</u> , further comprising: determining if connectivity between the server and the second device has been disrupted; and providing a notification by the application on the second device that the connectivity has been disrupted.	¶33; Claim 5 (p.28)
[31]	The method of claim <u>26</u> , wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.	Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35;
[32]	The method of claim <u>26</u> , 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.	¶45; ¶48;
[33]	The method of claim <u>26</u> , wherein the information received at the second device is a user's private cards in an online card game.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48;
[34]	The method of claim <u>26</u> , wherein the a display on the first device is being viewed exclusively by a first user and a display on a second device is also being viewed exclusively by the first user.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶35; ¶39; ¶45; ¶48; ¶57; ¶65; ¶78;
[35]	The method of claim <u>30</u> , 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	¶45; ¶48;

	indicator on the second device indicating a link between the information displayed on the respective devices.	
[36]	The method of claim <u>26</u> , wherein the server is a proxy server configured to relay communications from an application server to the first and second devices wherein the proxy server emulates a client to the application server.	¶50; ¶52;
[37]	The method of claim <u>26</u> , further comprising configuring the server for managing an online game, and wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, wherein the first electronic device is primarily used to play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.	¶23; ¶25; Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35; Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48;
[38]	The method of claim <u>37</u> , wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48;
[39]	The method of claim <u>26</u> , further comprising electronically storing at the server a parameter indicating whether subsets of the information are to be divided between two or more devices.	¶25-26; ¶31; ¶33-34; ¶35;
[40]	The method of claim <u>26</u> , wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.	¶20-23; ¶55 ¶57; ¶77-78
[41pre]	A system for transmitting information to multiple electronic devices, the system comprising:	¶2; ¶18-19; ¶23-25;
[41a]	an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶89-90;
[41b]	a processor device programmed for:	¶81; ¶98 ¶¶101-102

[41c]	identifying a first subset of the information and identifying a second subset of the information;	¶23-28; ¶38;
[41d]	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 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;	Fig. 10; ¶26; ¶33; ¶75; ¶83; ¶89; ¶90; ¶92
[41e]	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.	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; ¶23-29 ¶33-34; ¶58; 65; ¶78; ¶82;

IV. PERSON OF ORDINARY SKILL IN THE ART (POSITA).

Petitioner proposed level of skill is “a bachelor’s degree in electrical or computer engineering or computer science or a comparable field of study, plus approximately two years of professional experience in the field of computer and/or network design and security or other relevant industry experience.” *See* Paper 2 (“Pet.”) at 5. Patent Owner agrees with Petitioner that a POSITA would have two years of professional experience in the field of (i) computer and security, and/or (ii) network design and security. Ex. 2004, ¶39. The ’376 Patent is directed at security and securing online transactions from malware therefore it is appropriate that a POSITA have work

experience in security. Patent Owner objects to Petitioner’s use of the catchall “or other relevant industry experience” as vague and unhelpful. Ex. 2004, ¶39.

V. CLAIM CONSTRUCTION

In the Decision, the Board declined to expressly construe any claim terms. *See* Paper 10 (“Inst. Dec.”) at 14. Nor has Petitioner provided any explicit claim construction of any claim terms. In light of arguments made by Petitioner with respect to original claim 3, 16 and 17, Patent Owner believes it is necessary to propose a partial claim construction for the term “sensitive information” found in Substitute Claims 28, 30, 35, 37 and 38. In particular, Patent Owner proposes that “sensitive information” be construed to mean, at least in part, “information that will not be automatically shared with the first device.”

IPR proceedings apply “the *Phillips* claim construction standard governing federal courts.” *CUPP Computing AS v. Trend Micro Inc.*, 53 F. 4th 1376, 1380 (Fed. Cir. 2022); 37 C.F.R. § 42.100(b). The *Phillips* standard provides in relevant part:

Claim construction requires determining how a skilled artisan would understand a claim term in the context of the entire patent, including the specification. We begin by considering the language of the claims themselves. However, claims must be read in view of the specification, of which they are a part. We have explained that the specification is the single best guide to the meaning of a disputed term, and is, thus, the primary basis for construing the claims.

Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC, 57 F. 4th 1001,

1008 (Fed. Cir. 2023) (internal citations and quotations omitted) (quoting *Phillips v. AWH Corp.*, 415 F. 3d 1303, 1313 (Fed. Cir. 2005)).

The claims of the '376 Patent teach that “sensitive information” is information shared with the second device. Original claim 3 for example discloses sending “non-sensitive information” to the first device, and “sensitive information” to the second device. Ex. 1001, Col.15:43-45. Similarly, Original claim 16 discloses “the first electronic device is primarily used to play the game” and “sensitive information” is sent to the “second electronic device so that sensitive information can be presented to a user.” Ex. 1001, Col.16:35-39. The claims of the '376 Patent unmistakably teach that “sensitive information” is delivered to the second device.

The specification teaches that with respect to the claimed invention, “sensitive information” is information that an application practicing the '376 Patent should not automatically share with the first device out of concern the first device may be compromised by malware. In the online poker embodiment, the “game server does not communicate certain sensitive information (for example, the user’s hole cards) to the first device.” Ex. 2005, ¶23. The specification further explains “because the sensitive information is not displayed or transmitted to the first device, an attacker using malware cannot gain access to the sensitive information.” *Id.* The specification further describes the situation where the first device does not receive indication that the second device has received the users “hole cards.” Ex. 2005, ¶31. In that

situation, the user's turn is delayed and will be folded out. *Id.* However, the specification explains “[i]f the user notices that there is a problem with the second device not receiving the hole cards in time, and if this affects his ability to play the game, the user may elect to downgrade the user's security and to receive his hole cards on the first device, until such time as the problem is rectified.” Ex. 2005, ¶31; *see also* ¶¶34-37 (describing user electing to share sensitive information with first device)

This point is amplified by the specifications teaching that “sensitive information” can be shared with the first device once it is no longer considered “sensitive.” The common example is where a poker hand is completed the “hole cards” may be shared with the first device because their sensitivity has diminished: “[A]fter 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.” Ex. 2005, ¶40.

In sum, the claims together with teachings of the specification for the '376 Patent demonstrate that the claimed “sensitive information” in Substitute Claims 28, 30, 35, 37 and 38, is at minimum, information that is not automatically shared with the first device. Ex. 2004, ¶¶41-42.

VI. THE PROPOSED SUBSTITUTE CLAIMS ARE PATENTABLE OVER THE INSTITUTED GROUNDS AND ART.

The Substitute Claims distinguish the cited references relied upon in the

Board’s institution decision with respect to independent claims 1 and 25 (corresponding to Substitute Claims 26 and 41). Patent Owner does not bear the burden of proving the patentability of Substitute Claims 26-41. *See Lectrosonics*, Paper 15 at 3-4; *Aqua Prods., Inc. v. Matal*, 872 F. 3d 1290, 1295-96, 1327 (Fed. Cir. 2017) (*en banc*). Rather, Petitioners must prove unpatentability by a preponderance of the evidence. *See Lectrosonics*, Paper 15 at 4. However, Patent Owner provides the following comments regarding the Substitute Claims.

A. ZHA DOES NOT TEACH OR SUGGEST THE LIMITATIONS PROPOSED FOR THE SUBSTITUTE CLAIMS.

Zha (U.S. Patent 9,497,565) discloses a method for “displaying an interfaces, an apparatus, a terminal and a server.” Ex. 2004, ¶49. The “problem” identified by *Zha* is use of an application program with more than one “functional interface,” such as a “microblog”¹ with a “homepage interface,” a “private messaging interface” and a “game interface.” *Id.* If the user is using the homepage functional interface on their terminal, but wants to send a private message to a friend, the user must operate their terminal to exit the homepage functional interface and then enter the private message functional interface. *Id.* *Zha* explains that “[s]ince the application program may provide multiple functional interfaces” the user must operate their terminal to

¹ Well known microblogs that existed at the time *Zha* was published included Twitter, Facebook, Instagram, Tumblr, Reddit and LinkedIn. *See, e.g.*, Ex. 2007, A Guide through 7 Microblogging Websites, <https://www.linkedin.com/pulse/guide-through-7-microblogging-websites-realytviews/>

“switch” between the various functional interfaces the user desires to access. Ex. 2004, ¶49, Ex. 1004, Col.1:33-36. This “switching process” requires the terminal to download “related data from the server, thereby increasing a network traffic imperceptibly.” Ex. 2004, ¶49, Ex. 1004, Col.1:37-39. *Zha* states that when switching frequently amongst functional interfaces, the “user needs to operate the terminal to switch between different functional interfaces back and forth, thus an operational complexity for the user is high.” Ex. 1004, Col.1:39-43.

Zha further discloses a “method for displaying an interface . . . where the first terminal and a second terminal currently use an application program with one account.” Ex. 1004, Col.2:1-5; Ex. 2004, ¶50. *Zha* discloses using “access permissions for different functional interfaces . . . assigned to terminals which simultaneously use an application program with one account.” Ex. 1004, Col.2:59-63. *Zha* further discloses that “data corresponding to each of the functional interfaces is only assigned to a terminal having an access permission for the functional interface, instead of assigning the data corresponding to each of the functional interfaces to all the terminals using the application program.” Ex. 1004, Col.2:62-67.

According to *Zha*, this separation of data “solv[es] the problem that the consumption of network traffic is large in conventional technology and reducing the network traffic occupied in assigning the data corresponding to different functional interfaces to the terminals.” Ex. 2004, ¶50-51, Ex. 1004, Col.2:67-3:4. *Zha* adds that

“operational complexity for the user” is reduced by having multiple terminals receive only the data for their assigned functional interface and thus reducing the need for “frequent switching operations.” Ex. 2004, ¶50-51, Ex. 1004, Col.3:3-14.

Substitute Claim 26 (formerly original claim 1) requires “*using application specific authentication information* 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.*” Appendix A, pp. 3. *Zha* does not mention or disclose the use of authentication information to determine if a first user is logged into the application. Ex. 2004, ¶52. More specifically, *Zha* does not mention or disclose the use of authentication information that is “application specific” and that the application specific authentication information is different for determining login to the application at the first and second devices. Ex. 2004, ¶52.

Zha discloses generally that the “user may login to a microblog in the laptop computer, the cellphone and the desktop computer with one microblog account.” Ex. 2004, ¶53, Ex. 1004, Col.6:56-61. This generic discussion is repeated throughout *Zha*. Ex. 2004, ¶53, *see also*, Ex. 1004, Col.7:33-4. At most, *Zha* mentions generic “logging in” to two terminals with the same account but does not disclose using application specific authentication information to log into the application on the first and second device, or that the application specific authentication information is

different between the first device and second device. Ex. 2004, ¶ 54.

Substitute Claims 28, 30, 35, 37 and 38 all additionally require “sensitive information” is sent to the second device. *Zha* does not disclose sending “sensitive information” to the second device. Petition argues that *Zha*’s “private message interface data” corresponds to the “sensitive information” limitation in original claim 3. Ex. 1002, ¶¶99-100. This is wrong. Substitute Claim 26, on which Substitute Claims 28, 30, 35, 37 and 38 all depend, claims the “sensitive information” that is sent to the second device must be (i) *generated by the application* (ii) *at the server* and (iii) *specific to the application*. Ex. 2004, ¶63. *Zha*’s “private messages” sent via the microblog’s private message interface, are generated by the users (not the “same application”), on the user’s device (not the server), and private messages are not specific to any application. Ex. 2004, ¶63. Additionally, *Zha*’s “private messages” are not equivalent to “sensitive information” as claimed in Substitute Claims. *Zha*’s disclosure of a “private message application” as part of a microblog is simply describing the “direct messaging” (or “DM”) component of a microblog such as Facebook or Twitter. Ex. 2004, ¶64. *Zha* does not disclose “sensitive information” as that term is claimed and used in Substitute Claims 28, 30, 35, 37 and 38.

B. TSUSHIMA DOES NOT TEACH OR SUGGEST THE LIMITATIONS PROPOSED FOR THE SUBSTITUTE CLAIMS.

Tsushima (U.S. Patent Pub. 2014/0006485) is directed towards “a content providing system, a control method thereof, and particularly to a streaming

distribution technique for encoded video data.” Ex. 1010, ¶2. *Tsushima* states that its invention is a “content providing system” and “control method . . . that realizes a content service in which it is possible to provide a wide range of operation input to a user.” Ex. 1010, ¶11. Nothing in *Tsushima* relates to security and/or securing online transactions.

As noted above, Substitute Claim 26 (formerly original claim 1) requires “*using application specific authentication information* 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.*” Appendix A, p. 3. *Tsushima* does not disclose this limitation. Ex. 2004, ¶¶69-70. *Tsushima* discloses inputting of “account information for the user” at the first and second device to achieve successful login, however, nowhere does *Tsushima* disclose using different authentication information for logging into the first and second device. Ex. 1010, ¶57-59, 61; Ex. 2004, ¶¶66-70.

C. TAKAHASHI DOES NOT TEACH OR SUGGEST THE LIMITATIONS PROPOSED FOR THE SUBSTITUTE CLAIMS.

Takahashi (PCT/JP2012/007595) relates to “a technique for controlling game progress with a communications terminal of a user via a communications network.” Ex. 1007, ¶2. *Takahashi* states that the object of the invention is directed to a “game control device, a non-transitory computer readable recording medium, a game control method, and a game control system that allows a variety of types or forms of

games by use of a plurality of communications terminals.” Ex. 1007, ¶6. The “problem” identified by *Takahashi* is that a user of a social network games uses a “mobile communication terminal irrespective of where the user is” thus “it is difficult to realize a variety of types or forms of games on the assumption that the user uses a single communication terminal.” Ex. 1007, ¶5.

As noted above, Substitute Claim 26 (formerly original claim 1) requires “***using application specific authentication information*** 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.***” Appendix A, p. 3. *Takahashi* does not disclose this limitation.

Takahashi discloses a login process which is then followed separately by an authentication process, not a login process using authentication information as provided in the Substitute Claims. Ex. 2004, ¶¶90-91. For example, Figure 11 of *Takahashi* discloses a process where a registered user “logins to the game server,” but then teaches authentication after the user is logged in. Ex. 1007, ¶110, Fig. 11 (showing “Authentication processing” “after user logins.”). Accordingly, *Takahashi* does not disclose being logged into the application using application specific authentication information 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. Ex. 2004, ¶¶90-91. Only after the user “logs in to the game” does *Takahashi* disclose an authentication process, that uses “identification information, or the user ID and the password” to authenticate the user. Ex. 1007, ¶110; Ex. 2004, ¶¶90-91.

Furthermore, *Takahashi* states that “identification information” used by the mobile device for user authentication is “unique information for each mobile terminal.” Ex. 1007, ¶74. This is device specific authentication information, not application specific authentication information. Ex. 2004, ¶¶93-94. Every disclosed embodiment of *Takahashi* includes at least the use of one mobile device (*see, e.g.*, Ex. 1007, Fig. 1, 7-9, 15, 18, 20), meaning every authentication process in *Takahashi* involves the use of *device specific* authentication information and thus does not disclose the new limitations in Substitute Claims 26 and 41. Ex. 2004, ¶¶93-94. In no circumstance does *Takahashi* disclose using “application specific” only authentication information. *Id.* Moreover, even if *Takahashi* did disclose using two PCs with application specific authentication information, for example “user ID and password,” *Takahashi* does not disclose using different application specific authentication information for the first and second device. Ex. 2004, ¶¶94-95.

Substitute Claims 26 and 41 require a user to be logged in via an authentication process using application specific authentication information 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. Appendix A, pp. 3, 8.

Takahashi clearly discloses an authentication process that occurs after a user has logged into *Takahashi*'s game server. Ex. 2004, ¶¶91-92. Moreover, in all the various possible combinations of authentication using two devices, *Takahashi* does not disclose using application specific authentication information 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. Ex. 2004, ¶¶93-95.

Takahashi also fails to disclose “sensitive information” sent to the second device as required by Substitute Claims 28, 30, 35, 37 and 38. Petition argues that *Takahashi* discloses sending only “sensitive information” to the second device based on *Takahashi*'s disclosure of sending “user-specific information” to the *Takahashi*'s mobile device. Ex. 1002, ¶261. Petitioner argues that the user's “game results” could be “sensitive” information because “knowing another player's score could provide a player with an unfair advantage.” Ex. 1002, ¶262.

Takahashi's “game results” does not disclose “sensitive information” as that term would be understood by a POSITA. First, *Takahashi* relates to “social network games” that are “played among a plurality of unspecified users who are communicating with each other.” Ex. 1007, ¶0003. As to be expected with social

games, Takahashi discloses sharing “game results” amongst the users. Ex. 1007, ¶¶129, 135, 142; Ex. 2004, ¶104. This is not “sensitive information” as claimed in the ’376 Patent meant to be shielded from the first device to avoid exposure to malware.

Moreover, Takahashi’s “game results” will be shared automatically with Takahashi’s first device when a user plays a social game using only one device. Ex. 2004, ¶103. Whether a user practicing Takahashi starts with a single device, or starts with two devices and switches to a single device, Takahashi automatically, and predictably, shares “game results” with the first device. *Id.* However, as discussed above, “sensitive information” is information not automatically shared with the first device. *See* Section V (Claim Construction), *supra*. Accordingly, Takahashi fails to disclose sending “sensitive information” as claimed in Substitute Claims 28, 30, 35, 37 and 38, to the second device. Ex. 2004, ¶¶101-105.

D. ZHA, TSUSHIMA AND TAKAHASHI ARE NOT “ANALOGOUS” PRIOR ART.

Petitioner’s reliance on *Zha*, *Tsushima* and *Takahashi* is misplaced because none are “analogous” prior art. Prior art is considered “analogous” where: (1) the reference is from the same field of endeavor as the claimed invention or (2) the reference is reasonably pertinent to the problem faced by the inventor. *See* MPEP § 2141.01(A). The “‘same field of endeavor’ and ‘reasonably pertinent’ are two separate tests for establishing analogous art; it is not necessary for a reference to

fulfill both tests in order to qualify as analogous art.” MPEP § 2141.01(A); *see also*, *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019). *Zha*, *Tsushima* and *Takahashi* are all from different fields of endeavor, and all seek to solve much different problems than the ’376 Patent. Ex. 2004, ¶¶57, 58, 72-75, 96-98.

The field of endeavor for the ’376 Patent is online security. Dr. Rubin’s personal background as professor emeritus at Johns Hopkins University in the field of computer security. Ex. 2004, ¶56. More specifically, the ’376 Patent states that the field of invention relates to “securing communications against malware by utilizing two devices with differential or application-specific component during an online session.” Ex. 2005, ¶2. This is supported by the claims which claim use of applications designed to use two device, and only when the user is authenticated on both devices, transmit select data to only one of the two devices in case malware has compromised the other device. *See, e.g.*, Ex. 2005, pp. 27-28 (original proposed Claims 1 and 3). Further, the problem the ’376 Patent seeks to solve are the shortcomings of two-factor authentication. Ex. 2004, ¶58. The ’376 Patent discloses a system and method where “the user has persistent use of a first device and a second device throughout the use of an online application ***to prevent a compromise of the transaction if malware infects either device.***” Ex. 2005, ¶18 (emphasis added); Ex. 2004, ¶58.

Zha is directed towards “interface display” on multiple terminals, and

specifically to online applications with more than one functional interface. Ex. 2004, ¶57. Nothing in *Zha* relates to the field of online security generally, or securing communications against malware more specifically. Ex. 2004, ¶57. *Zha* attempts to solve a much different problem than '376 Patent. As discussed above, *Zha* assigns different access permissions for applications with more than one functional interface so that each terminal only receives data specific to its assigned functional interface. Ex. 2004, ¶58. According to *Zha*, this helps to reduce (i) network traffic and (ii) switching by the user. Ex. 2004, ¶58. Because *Zha* pertains to a different “field of endeavor” and attempts to solve a different problem than the '376 Patent, *Zha* is not analogous prior art.

Tsushima is directed towards “a content providing system, a control method thereof, and particularly to a streaming distribution technique for encoded video data.” Ex. 1010, ¶2. *Tsushima* states “[t]he present invention relates to a content providing system and a control method, and particularly to a technique of loading static data into shared memory.” *Id.* *Tsushima*’s “Summary of Invention” describes inventing a “content providing system, and a control method thereof, that realizes a content service in which it is possible to provide a wide range of operation input to a user.” Ex. 1010, ¶11. *Tsushima* is focused on improving upon conventional techniques of experiencing streaming video data whether from network games or a “video distribution service.” Nothing in *Tsushima* relates to online security generally,

or securing communications against malware more specifically. Ex. 2004, ¶76.

Tsushima is also directed to a much different problem than '376 Patent.

Tsushima seeks to provide a wider range of “operational inputs” for a user when using a mobile device as the controller for a video display (whether a game or a video) on a separate “display device.” Ex. 1010, ¶¶10-11. Because *Tsushima* pertains to a different “field of endeavor” and attempts to solve a different problem than the '376 Patent, *Tsushima* is not analogous prior art. Ex. 2004, ¶¶72-78.

Takahashi is directed to “a game control device” for online games and has nothing to do with securing online activities from potential malware. Ex. 2004, ¶97. *Takahashi*'s field of endeavor relates to techniques “for controlling game progress with a communications terminal.” *Id.*; Ex. 1007, ¶2. While the preferred embodiment of the '376 Patent is directed to “online games,” the invention can be applied to any number of online activities “such as online banking, mobile healthcare, online investing, and other online activities that would benefit from enhanced security against malware on a user's computing device.” Ex. 2005, ¶20. Accordingly, a POSITA would not look broadly to “online games”, “online banking”, “mobile healthcare”, “online investing” and “other online activities” for prior art relevant to the '376 Patent, unless the prior art was also directed to enhancing security. Ex. 2004, ¶96. Otherwise, the field of endeavor would be so broad (i.e., online computing) as to be meaningless in terms of defining the bounds of relevant prior art.

Id. Further, Takahashi’s game control techniques are meant for applications utilizing one, or two, devices, where the ’376 Patent is directed to applications for use exclusively with two devices. Ex. 2004, ¶97.

Finally, *Takahashi* attempts to address the “problem” that a user of a social network games uses a “mobile communication terminal irrespective of where the user is” and as a result “it is difficult to realize a variety of types or forms of games on the assumption that the user uses a single communication terminal.” Ex. 1007, ¶5, Ex. 2004, ¶88. This is completely unrelated to the problems addressed in the ’376 Patent. Ex. 2004, ¶98. Accordingly, because *Takahashi* pertains to a different “field of endeavor” and attempts to solve a different problem than the ’376 Patent, *Takahashi* is not analogous prior art.

E. THERE IS NO MOTIVATION TO COMBINE.

There is no motivation to combining *Zha* or *Takahashi* with the general knowledge of a POSITA, or to combine *Zha* or *Takahashi* with *Tsushima*. Each reference is extremely far afield from the field of endeavor for the ’376 Patent, and each seeks to address an unrelated problem.

Zha is limited to online applications with different functional interfaces, essentially microblogs. Ex. 2004, ¶¶60-61. As noted in every claim of *Zha*, an application program must have a “functional interface to the first terminal being distinct at least in part from the assigned functional interface assigned to the second

terminal.” *Id.*; *see also* Ex. 1004, Col. 29:31-33. This makes sense for *Zha* because unless an application program has more than one functional interface to choose from, there is no reason to apply the teachings of *Zha* in order to reduce the network traffic or lower the amount of switching between functional interfaces to decrease “operational complexities.” Ex. 2005, ¶¶60-61. A POSITA would not look far afield to *Zha* which is directed to a very small subset of applications in order to achieve the claims of the ’376 Patent which have a much broader application in the field of online security. *Id.*

Similar to *Zha*, *Tsushima* is narrow in its application within its own field of endeavor. *Tsushima*’s disclosure requires very specific first and second devices while the ’376 Patent is device agnostic. Ex. 2004, ¶80. Moreover, *Tsushima* is limited to video processing applications (such as games or “video on demand”) where the server performs the processing. Ex. 2004, ¶82. A POSITA would not look to combine two reference (i) so far afield from each other and ’376 Patent, (ii) which are extremely narrow in application within their respective fields of endeavor, and (iii) solve totally different problems. Ex. 2004, ¶¶79-85.

With the exception of being an online game, there is no reasonable basis why a POSITA would look to combine *Takahashi* with the general knowledge of a POSITA or with *Tsushima*. *Takahashi* has nothing to do with security, or securing online transactions. Ex. 2004, ¶¶99-100. Moreover, *Takahashi* seeks to improve social

gaming experience whether the user plays one or two devices compared to '376 Patent which relies exclusively on two devices. Furthermore, *Takahashi* always requires use of a mobile device where '376 Patent is device agnostic. *Id.* There is simply no teaching or suggestion in *Takahashi* that would lead a POSITA to take the disclosure for a game controller requiring at least one mobile device and combine it with a POSITA's general knowledge, or *Tsushima*, to achieve the claims of the '376 Patent. *Id.*

VII. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests the Board grant this motion, cancel claims 1-5, 9-10, 12-17, and 23-25 and substitute claims 26-41 as set forth in Appendix A.

Dated: December 1, 2023

/Robert S. McArthur/

Robert S. McArthur, Esq.
Registration No. 45,674
VASQUEZ BENISEK & LINDGREN LLP
1550 Parkside Drive, Ste 130
Walnut Creek, CA 94596
Main Telephone (925) 637-4250
Direct Telephone (415) 699-0630
Main Facsimile (925) 403-0900
mcarthur@vblaw.com
Counsel for Patent Owner

APPENDIX A

LISTING OF CLAIMS

Patent Owner presents the following non-contingent substitute claims.

Pursuant to 37 C.F.R. § 1.121(c)(2), the use of strikethroughs/brackets indicate deleted text and underlining indicates inserted text.

Listing of Claims:

Claims 1-5 (canceled)

6. (not challenged) The method of claim 5, further comprising determining by an absence of a heartbeat if the connectivity has been disrupted and receiving an election from the user whether or not to switch to using only the first device for subsequent communications.

7. (not challenged) The method of claim 1, further comprising:
detecting whether the second device has received the second subset of the information;

displaying the second subset of the information on the second device; and
generating an indicator on the first device indicating that the second device has received the second subset of the information.

8. (not challenged) The method of claim 7, wherein if the first device has not received the indication that the second device has received the second subset of the information, then a user's turn in an online game is delayed.

Claims 9-10. (canceled)

11. (not challenged) The method of claim 10, wherein the information linked at the second device comprises hole cards and the information linked at the first device comprises community cards in a hand in a game of poker.

Claims 12-17. (canceled)

18. (not challenged) The method of claim 17, wherein the first device provides a visual mark on each of multiple tables that is displayed that matches a visual mark on the hole cards that are displayed on the second device to keep the hole cards and the tables synchronized.

19. (not challenged) The method of claim 17, wherein the game server provides information to identify the table to which table the hole cards belong.

20. (not challenged) The method of claim 17, wherein the first device communicates to the game server which table has focus, and wherein the game server then communicates to the second device an instruction to display the hole cards that correspond to an active table that has the focus in the first device.

21. (not challenged) The method of claim 17, wherein a user is playing more than one poker table, and wherein the first device communicates to the second device information indicating which hole cards to view on the second device corresponding to an active table having focus on the first device.

22. (not challenged) The method of claim 1, wherein the set of information at a server represents financial record information and the first subset of the information comprises account identifying information and the second subset of the information comprises account balance information.

Claims 23-25. (cancelled)

[[1.]] 26. (Substitute for Claim 1) A method for transmitting information to multiple electronic devices, the method comprising:

electronically storing a set of information at a server;

identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;

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 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;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting [[a]] the first subset of the information to the first device from the server; and

transmitting [[a]] 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.

[[2.]] 27. (Substitute to Claim 2) The method of claim [[1]] 26, further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.

[[3.]] 28. (Substitute for Claim 3) The method of claim [[1]] 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information.

[[4.]] 29. (Substitute for Claim 4) The method of claim [[1]] 26, wherein the information received at the second device is more sensitive than the information received at the first device.

[[5.]] 30. (Substitute for Claim 5) The method of claim [[1]] 28, further comprising:

determining if connectivity between the server and the second device has been disrupted; and

providing a notification by the application on the second device that the connectivity has been disrupted.

[[9.]] 31. (Substitute for Claim 9) The method of claim [[1]] 26, wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.

[[10.]] 32. (Substitute for Claim 10) The method of claim [[1]] 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.

[[12.]] 33. (Substitute for Claim 12) The method of claim [[1]] 26, wherein the information received at the second device is a user's private cards in an online card game.

[[13.]] 34. (Substitute for Claim 13) The method of claim [[1]] 26, wherein the a display on the first device is being viewed exclusively by a first user and a display on a second device is also being viewed exclusively by the first user.

[[14.]] 35. (Substitute for Claim 14) The method of claim [[1]] 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.

[[15.]] 36. (Substitute for Claim 15) The method of claim [[1]] 26, wherein the server is a proxy server configured to relay communications from an application server to the first and second devices wherein the proxy server emulates a client to the application server.

[[16]] 37. (Substitute for Claim 16) The method of claim [[1]] 26, further comprising configuring the server for managing an online game, and wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, wherein the first electronic device is primarily used to play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.

[[17.]] 38. (Substitute for Claim 17) The method of claim [[16]] 37, wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.

[[23.]] 39. (Substitute for Claim 23) he method of claim [[1]] 26, further comprising electronically storing at the server a parameter indicating whether subsets of the information are to be divided between two or more devices.

[[24.]] 40. (Substitute for Claim 24) The method of claim [[1]] 26, wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.

[[25.]] 41. (Substitute for Claim 25) A system for transmitting information to multiple electronic devices, the system comprising:

an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;

a processor device programmed for:

identifying a first subset of the information and identifying a second subset of the information;

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 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;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting [[a]] the first subset of the information to the first device from the server; and

transmitting [[a]] 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.

CERTIFICATE OF FILING AND SERVICE

I hereby certify that a true and correct copy of the foregoing PATENT OWNER'S MOTION TO AMEND is being filed electronically via PTAB E2E and served on counsel for Petitioner by electronic mail this 1st day of December, 2023 as follows:

R. William Beard, Jr. (wbeard@sgbfirm.com)
Brian C. Banner (bbanner@sgbfirm.com)
SLAYDEN GRUBERT BEARD PLLC
401 Congress Avenue, Suite 1650
Austin, Texas 78701
litigation@sgbfirm.com

Dated: December 1, 2023

/Robert S. McArthur/
Robert S. McArthur, Esq.
Registration No. 45,674
VASQUEZ BENISEK & LINDGREN LLP
1550 Parkside Drive, Ste 130
Walnut Creek, CA 94596
Main Telephone (925) 637-4250
Direct Telephone (415) 699-0630
Main Facsimile (925) 403-0900
mcarthur@vblaw.com
Counsel for Patent Owner