

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

**SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.,**
Petitioners

v.

MAXELL CORPORATION,
Patent Owner

Inter Partes Review No.: IPR2025-01307
U.S. Patent No. 11,026,088

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. U.S. 11,026,088 UNDER 35 U.S.C. §§ 311-319
AND 37 C.F.R. §§ 42.1-100, ET SEQ**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	12
II. STATEMENT OF PRECISE RELIEF REQUESTED	12
III. THE '088 PATENT	12
A. Summary of the '088 Patent.....	12
B. Priority Date of the '088 Patent.....	16
IV. SUMMARY OF PRIOR ART.....	16
A. Iwami (EX1004/EX1005)	16
B. Kim (EX1006).....	17
C. Weiser (EX1008).....	17
D. Kato (EX1009)	17
E. Liansky (EX1012)	18
F. Dowling (EX1013).....	18
V. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3).....	18
A. Person of Ordinary Skill in the Art	18
B. Claim Construction Standards.....	18
1. “access point device” (claims 1, 14, 15).....	19
2. Limitation [6b]	19
VI. GROUND 1: CLAIMS 1, 5 AND 13-15 ARE OBVIOUS OVER IWAMI IN VIEW OF KIM.....	20
A. Proposed Combination and Motivation to Combine.....	20
B. Claim 1	24
1. [1pre]	24
2. [1a]	24
3. [1b]	26
4. [1c]	27
5. [1d]	32
6. [1e]	37

7.	[1f].....	38
C.	Claim 5	41
1.	[5a]	41
2.	[5b]	43
D.	Claim 13	45
1.	[13a]	45
2.	[13b]	46
E.	Claim 14	47
1.	[14pre].....	47
2.	[14a]	47
3.	[14b]	48
4.	[14c]	48
5.	[14d]	48
6.	[14e]	48
F.	Claim 15	48
1.	[15pre].....	48
2.	[15a]	48
3.	[15b]	49
4.	[15c]	49
5.	[15d]	49
6.	[15e]	49
7.	[15f].....	50
VII.	GROUND 2: CLAIMS 2 AND 12 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY	50
A.	Proposed Combination and Motivation to Combine.....	50
B.	Claim 2	52
1.	[2pre], [2a]	52
C.	Claim 12	55
1.	[12a]	55

2.	[12b]	55
3.	[12c]	56
VIII.	GROUND 3: CLAIMS 7, 8, AND 10 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY AND WEISER.....	58
A.	Proposed Combination and Motivation to Combine.....	58
B.	Claim 7	60
1.	[7a]	60
2.	[7b]	61
3.	[7c]	62
4.	[7d]	62
5.	[7e]	63
6.	[7f].....	64
7.	[7g]	64
C.	Claim 8	65
1.	[8a]	65
2.	[8b]	66
3.	[8c]	66
4.	[8d]	67
5.	[8e]	68
6.	[8f].....	68
7.	[8g]	69
D.	Claim 10	70
1.	[10a]	70
2.	[10b]	70
3.	[10c]	71
4.	[10d]	71
5.	[10e]	71
6.	[10f].....	72
7.	[10g]	73

IX.	GROUND 4: CLAIMS 9 AND 11 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY AND KATO	74
A.	Proposed Combination and Motivation to Combine.....	74
B.	Claim 9	76
1.	[9a]	76
2.	[9b]	78
3.	[9c]	79
C.	Claim 11	80
1.	[11a]	80
2.	[11b]	82
3.	[11c]	82
X.	GROUND 5: CLAIM 6 IS OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF DOWLING	82
A.	Motivation to Combine	82
B.	Claim 6	84
1.	[6a]	84
2.	[6b]	84
XI.	MANDATORY NOTICES UNDER 37 C.F.R. §§ 42.8(B)(1)-(4).....	85
A.	Real Parties-In-Interest.....	85
B.	Related Matters.....	85
C.	Lead and Backup Counsel.....	85
D.	Service Information	85
XII.	CONCLUSION.....	86

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Maxell Ltd. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 5:25-cv-00052-RWS (E.D. Tex.).....	86
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	20
Statutes	
35 U.S.C. § 103.....	13
35 U.S.C. § 311.....	13
Other Authorities	
37 C.F.R. § 42.8(B)(1)	86
37 C.F.R. § 42.8(B)(2)	86
37 C.F.R. § 42.8(B)(3)	86
37 C.F.R. § 42.8(B)(4)	86
37 C.F.R. § 42.104(a).....	13
37 C.F.R. § 42.104(B)(3)	19
AIA § 102.....	18, 19
AIA § 102(d)(2)	18

INDEX OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 11,026,088
1002	File History of U.S. Patent No. 11,026,088
1003	Declaration of Joseph A. Paradiso in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 11,026,088
1004	U.S. Patent Publication No. 2019/0053149 (“Iwami”)
1005	Certified Translation of Japanese Application No. 2014-024016
1006	U.S. Patent Publication No. 2007/0005788 (“Kim”)
1007	Certified Translation of Korean Application No. 10-2003-0065676
1008	U.S. Patent Publication No. 2013/0147900 (“Weiser”)
1009	U.S. Patent Publication No. 2015/0007302 (“Kato”)
1010	Certified Translation of Japanese Application No. 2013-134146
1011	Certified Translation of Japanese Application No. 2014-006624
1012	U.S. Patent No. 9,323,713 (“Liansky”)
1013	U.S. Patent Publication No. 2005/0036509 (“Acharya”)
1014	U.S. Patent Publication No. 2014/0233443 (“Kumar”)
1015	U.S. Patent Publication No. 2004/0267981 (“Kakemura”)
1016	U.S. Patent Publication No. 2015/0327310 (“Miura”)
1017	U.S. Patent Publication No. 2010/0323682 (“Hatayama”)
1018	U.S. Patent Publication No. 2013/0221084 (“Doss”)
1019	Microsoft Computer Dictionary (5th ed. 2002)
1020	Newton’s Telecom Dictionary (30th ed. 2016)
1021	U.S. Patent No. 6,636,499 (“Dowling”)

CHART OF CLAIMS	
[1pre]	A communication system comprising:
[1a]	a communication device;
[1b]	an access point device;
[1c]	a first communication terminal configured to connect to the communication device via the access point device and transmit a command to remotely control a display operation on the communication device connected with the first communication terminal; and
[1d]	a second communication terminal configured to, if having permission from the first communication terminal, establish a connection with the communication device to use the communication device;
[1e]	wherein, while the communication device outputs data received from the second communication terminal that has established the connection with the communication device and upon receiving, by the communication device, the command from the first communication terminal, the communication device is configured to control how to display the data received from the second communication terminal while maintaining the connection with the second communication terminal, and
[1f]	wherein, when the communication device receives information to terminate the permission from the first communication terminal, the communication device is configured to terminate the connection with the second communication terminal in accordance with the information to terminate permission received from the first communication terminal.
[2pre]	The communication system according to claim 1, wherein,
[2a]	for the permission, the first communication terminal transmits, to the second communication terminal, connection information necessary for a connection through short range communication with the second communication terminal, and the second communication terminal connects to the communication device by using the connection information.
[5pre]	The communication system according to claim 1, wherein,
[5a]	the first communication terminal displays information whether to terminate the permission on a display screen,
[5b]	receives an input operation for terminating the permission, and transmits the information to terminate the permission to the communication device in accordance with the input operation for terminating the permission.
[6pre]	The communication system according to claim 1, wherein,
[6a]	in a case that the communication device is able to receive information from the first communication terminal, the communication device controls the

CHART OF CLAIMS
communication device in accordance with information from the first communication terminal,
[6b] wherein, in a case that the communication device is unable to receive information from the first communication terminal, the communication device terminates the connection with the second communication terminal.
[7pre] The communication system according to claim 1, wherein,
[7a] for the permission, the first communication terminal transmits, to the second communication terminal, connection information necessary for a connection through short range communication with the second communication terminal, and
[7b] the second communication terminal transmits address information on the second communication terminal to the first communication terminal,
[7c] the first communication terminal transmits the address information on the second communication terminal to the communication device,
[7d] the communication device registers the address information on the second communication terminal into a permission list,
[7e] the second communication terminal connects to the communication device by using the connection information,
[7f] upon confirming the permission is to be terminated, the first communication terminal causes the communication device to delete the address information on the second communication terminal from the permission list of the communication device, and,
[7g] upon the address information on the second communication terminal being not registered in the permission list, the communication device terminates the connection with the second communication terminal.
[8pre] The communication system according to claim 1, wherein,
[8a] for the permission, the first communication terminal transmits, to the second communication terminal, connection information necessary for a connection through short range communication with the second communication terminal, and
[8b] the second communication terminal transmits address information on the second communication terminal to the first communication terminal,
[8c] the first communication terminal registers the address information on the second communication terminal into a permission list,
[8d] the second communication terminal connects to the communication device by using the connection information,

CHART OF CLAIMS	
[8e]	upon confirming the permission is to be terminated, the first communication terminal causes the communication device to delete the address information on the second communication terminal from the permission list, and
[8f]	the communication device performs communication for confirmation with the first communication terminal and,
[8g]	upon the address information on the second communication terminal being not registered in the permission list of the communication device, terminates the connection with the second communication terminal.
[9pre]	The communication system according to claim 1, wherein,
[9a]	for the permission, the first communication terminal requests a one-time password from the communication device, and the communication device responds with the one-time password,
[9b]	the first communication terminal transmits, to the second communication terminal, connection information including the one-time password necessary for a connection through short range communication with the second communication terminal, and
[9c]	the second communication terminal connects to the communication device by using the connection information including the one-time password.
[10pre]	The communication system according to claim 1, wherein,
[10a]	for the permission, the second communication terminal performs short range communication with the communication device,
[10b]	the communication device transmits, to the second communication terminal, connection information necessary for a connection, and
[10c]	the second communication terminal transmits address information on the second communication terminal to the communication device,
[10d]	the communication device registers the address information on the second communication terminal into a permission list,
[10e]	the second communication terminal connects to the communication device by using the connection information,
[10f]	upon confirming the permission is to be terminated, the first communication terminal causes the communication device to delete the address information on the second communication terminal from the permission list of the communication device, and,
[10g]	upon the address information on the second communication terminal being not registered in the permission list, the communication device terminates the connection with the second communication terminal.
[11pre]	The communication system according to claim 1, wherein,

CHART OF CLAIMS
[11a] for the permission, the second communication terminal requests a one-time password from the communication device through short range communication with the communication device, and
[11b] the communication device transmits connection information including the one-time password necessary for a connection to the second communication terminal, and
[11c] the second communication terminal connects to the communication device by using the connection information including the one-time password.
[12pre] The communication system according to claim 1, wherein,
[12a] for the permission, the first communication terminal transmits, to the second communication terminal, connection information necessary for a connection through short range communication with the second communication terminal,
[12b] the second communication terminal connects to the communication device by using the connection information, and
[12c] in the short range communication, the first communication terminal displays a bar code representing the connection information on a display screen thereof and the second communication terminal captures an image of the bar code with a camera to read the connection information.
[13pre] The communication system according to claim 1, wherein,
[13a] the second communication terminal controls the communication device while maintaining the connection with the communication device, and
[13b] the first communication terminal controls the communication device while maintaining the connection with the communication device via the access point.
[14pre] A communication terminal comprising:
[14a] a wireless connection interface configured to connect to a communication device via an access point device; and
[14b] a controller configured to control the wireless connection interface and to transmit a command to remotely control a display operation on the communication device connected with the communication terminal,
[14c] wherein the controller is configured to transmit permission to establish a connection for the communication device and another communication terminal,
[14d] wherein, while the communication device outputs data received from the another communication terminal that has established the connection with the communication device, the controller is configured to transmit the command to control how to display the data while the communication device and the another communication terminal are connected, and

CHART OF CLAIMS
[14e] wherein, when the controller transmits information to terminate the permission from the communication terminal, the controller is configured to transmit the information to terminate the connection with the another communication terminal to the communication device.
[15pre] A communication device comprising:
[15a] a wireless connection interface configured to connect to a communication terminal and another communication terminal; and
[15b] a controller configured to control the wireless connection interface,
[15c] wherein the wireless connection interface is configured to connect to the communication terminal via an access point device,
[15d] wherein the controller is configured to control to establish a connection with the another communication terminal, if having permission from the communication terminal, and control data received from the another communication terminal,
[15e] wherein, while the controller controls the data received from the another communication terminal and upon receiving at the wireless communication interface, from the communication terminal, a command to remotely control how the data received from the another communication terminal is displayed, the controller is configured to control the data received from the another communication terminal in accordance with the command from the communication terminal while maintaining the connection with the another communication terminal, and
[15f] wherein, when the wireless communication interface receives information to terminate the permission from the communication terminal, the controller is configured to terminate the connection with the another communication terminal.

I. INTRODUCTION

In accordance with 37 C.F.R. § 42.104(a), Petitioner certifies that U.S. Patent 11,026,088 (the '088 patent) is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in this Petition.

II. STATEMENT OF PRECISE RELIEF REQUESTED

In accordance with 35 U.S.C. § 311, Petitioner requests cancellation of claims 1, 2, and 5-15 of the '088 patent (the “Challenged Claims”) in view of the following grounds:

Ground	Claims	Stat. Basis	Prior Art
1	1, 5, 13-15	35 U.S.C. § 103	Iwami and Kim
2	2, 12	35 U.S.C. § 103	Iwami, Kim and Liansky
3	7, 8, 10	35 U.S.C. § 103	Iwami, Kim, Liansky and Weiser
4	9, 11	35 U.S.C. § 103	Iwami, Kim, Liansky and Kato
5	6	35 U.S.C. § 103	Iwami, Kim and Dowling

III. THE '088 PATENT

A. Summary of the '088 Patent

The '088 patent is directed to a “wireless LAN communication system which achieves convenience where a terminal of a user who is external to an organization can temporarily use the system while ensuring security.” EX1001, Abstract. The '088 patent describes an organization, such as a company, with a wireless LAN communication system. Users within the organization may connect

their terminals to the wireless LAN communication system. EX1001, 1:14-23;
EX1003, ¶16.

The '088 patent explains that sometimes a user external to the organization may connect their terminal to the wireless LAN communication system. For example, a user within the organization can grant temporary access to a user outside the organization. The '088 patent notes that this creates a possible security problem where the external user can access the wireless LAN communication system later, after the temporary access was granted. The '088 patent aims to provide a solution where an external user terminal can conveniently connect to the wireless LAN communication system while ensuring security. EX1001, 1:47-2:10; EX1003, ¶17.

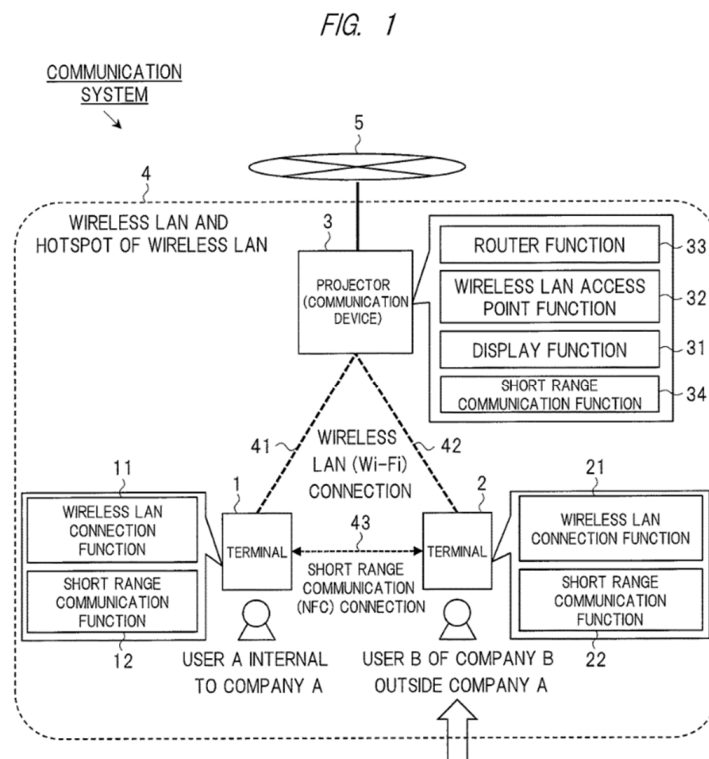


FIG. 1 of the '088 patent shows the basic configuration of the purported solution. FIG. 1 shows a communication system that includes terminal 1, also referred to as a “first communication device,” terminal 2, also referred to as a “second communication device,” and projector 3, also referred to as a “communication device.” Terminal 1 is a terminal of user A, a user internal to company A, while terminal 2 is a terminal of user B, a user outside company A. Projector 3, serving “both as a projection type display device and a communication device serving as an access point of the wireless LAN 4,” communicates with terminal 1 and terminal 2 by connections 41 and 42 established by wireless LAN 4. Terminal 1 and terminal 2 can also communicate with one another by near field communication (NFC) connection 43. EX1001, 3:44-5:8; EX1003, ¶18.

Being internal to company A, terminal 1 can connect to projector 3 by connection 41 and transmit data to projector 3, causing the display function 31 of projector 3 to display the data on a screen. Terminal 2 can connect to projector 3 by connection 42 and transmit data to projector 3, causing the display function 31 of projector 3 to display the data on the screen. However, because it is external to company A, terminal 2 connects and sends data to projector 3 under permission from terminal 1. EX1001, 5:9-22; EX1003, ¶19.

FIG. 2

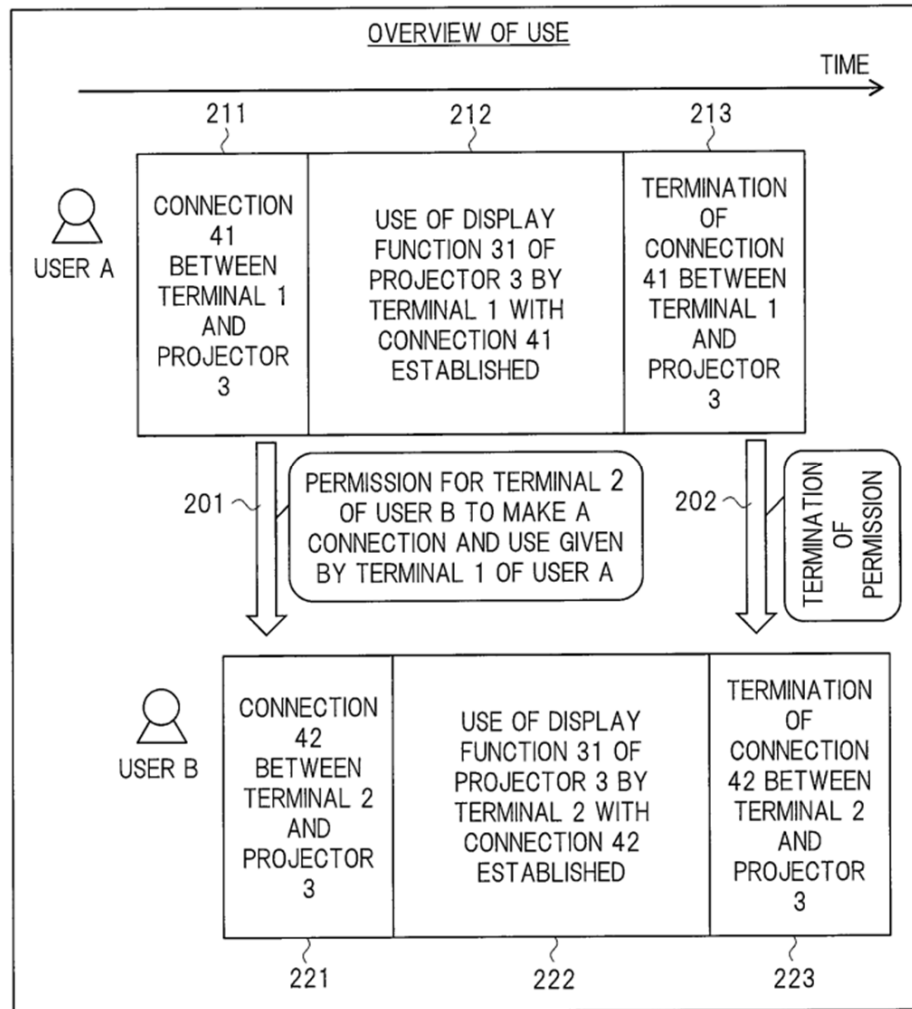


FIG. 2 shows an overview of the process. At 211, terminal 1, the internal terminal, connects to projector 3 through connection 41. Over time, terminal 1 uses display function 31 of projector 3 through connection 41 at 212 and, eventually, terminates connection 41 at 213. EX1001, 6:21-33; EX1003, ¶20.

While terminal 1 is connected to projector 3, at 201, user A of terminal 1 gives permission to terminal 2 (the external terminal) of user B to connect to projector 3. At 221, under the permission granted by user A, terminal 2 connects to

projector 3 through connection 42. Terminal 2 uses display function 31 of projector 3 through connection 42 at 222. At 202, terminal 1 terminates permission of terminal 2, thereby terminating connection 42 between terminal 2 and projector 3 at 223. EX1001, 6:34-67; EX1003, ¶21.

The '088 patent also discusses that terminal 1 can also be used as a “remote controller” of projector 3, for example controlling the display operation of the display function 31 to start or stop a video. EX1001, 9:41-53. However, contrary to the requirements of claim 1, there is no disclosure in this passage that terminal 1 can cause a video being supplied to the projector 3 by *another* terminal (such as terminal 2) to start or stop. EX1003, ¶22.

B. Priority Date of the '088 Patent

U.S. Application No. 15/504,668 was filed on 2/17/2017 as a national stage entry of PCT/JP2014/072783, filed 8/29/2014, which is therefore the earliest possible priority date. EX1001, front cover.

IV. SUMMARY OF PRIOR ART

A. Iwami (EX1004/EX1005)

Iwami was filed as U.S. Application No. 16/164,839 on 10/19/2018 and published as U.S. Patent Publication No. 2019/0053149 on 2/14/2019. EX1004, front cover. U.S. Application No. 16/164,839 claims priority to Japanese Application No. 2014-024016, filed 2/12/2014. EX1004, (30). All portions of Iwami EX1004 are present in the certified translation of Japanese Application No.

2014-024016, (EX1005). EX1003, ¶33. Thus, Iwami is effective as prior art as of 2/12/2014 under post-AIA §102(d)(2).

B. Kim (EX1006)

Kim was filed as U.S. Application No. 10/573,396 on 3/22/2006 and published as U.S. Patent Publication No. 2007/0005788 on 1/4/2007. EX1006, front cover. U.S. Application No. 10/573,396 claims priority to PCT/KR04/02422, filed 9/21/2004 and Korean Application No. 10-2003-0065676, filed 9/22/2003. EX1006, front cover. Kim is prior art under post-AIA §102.

C. Weiser (EX1008)

Weiser was filed as U.S. Application No. 13/313,940 on 12/11/2007 and published as U.S. Patent Publication No. 2013/0147900 on 6/13/2013. EX1008, front cover. Weiser is prior art under post-AIA §102.

D. Kato (EX1009)

Kato was filed as U.S. Application No. 14/306,653 on 6/17/2014 and published as U.S. Patent Publication No. 2015/0007302 on 1/1/2015. EX1009, front cover. U.S. Application No. 14/306,653 claims priority to Japanese Application No. 2013-134146, filed 6/26/2013, and Japanese Application No. 2014-006624. EX1009, front cover. Kato is prior art under post-AIA §102.

E. Liansky (EX1012)

Liansky was filed as U.S. Application No. 13/676,252 on 11/14/2012 and issued as U.S. Patent No. 9,323,713 on 4/26/2016. EX1012, front cover. Liansky is prior art under post-AIA §102.

F. Dowling (EX1021)

Dowling was filed as U.S. Application No. 09/453,163 on December 2, 1999 and issued as U.S. Patent No. 6,636,499 on October 21, 2003. EX1021, front cover. Dowling is prior art under post-AIA §102.

V. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)

A. Person of Ordinary Skill in the Art

A person of ordinary skill in the art at the time of the alleged invention of the '088 patent (8/29/2014) (“POSITA”) would have had a Bachelors’ degree in Electrical or Computer Engineering or a comparable field of study, plus approximately two to three years of professional experience with wireless LAN communications systems and distribution of information over the same, or other relevant industry experience. Additional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education. EX1003, ¶54

B. Claim Construction Standards

Any claim terms not listed below should be construed according to their plain and ordinary meaning to a POSITA at the time of the '088 patent. Petitioners

do not contend that its proposed constructions are complete constructions of these limitations or the claims for any other purpose, including issues that have been raised in the related litigation. Because the prior art asserted herein discloses the preferred embodiment within the indisputable scope of the claims, the Board need not construe the outer bounds of the claims as part of these proceedings. The district court may have to address other bounds of the claims in addressing infringement. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

1. “access point device” (claims 1, 14, 15)

This term means “in a wireless LAN (local area network), a transceiver that connects the LAN to a wired network.” EX1019 (Microsoft Computer Dictionary, 5th ed, 2002) (definition of “access point”); *see also* EX1020 (Newton’s Telecom Dictionary, 30 ed. 2016) at 112))(defining “access point” as “[n]etwork device that connects a wireless radio network to a wired LAN (local area network).”). This is the plain meaning to a POSITA in view of the ’088 patent specification. EX1003, ¶52.

2. Limitation [6b]

Limitation [6b] does not include any requirement for the communication device to terminate the connection with the second communication terminal *in response to or as a result of* the communication device being unable to receive

information from the first communication terminal. Moreover, [6b] does not limit what kind of information the communication device must be unable to receive in the “case.” Thus, [6b] is satisfied if the communication device terminates a connection with the second communication terminal during a time period when the communication device is unable to receive any kind of information from the first communication terminal. EX1003, ¶53.

VI. GROUND 1: CLAIMS 1, 5 AND 13-15 ARE OBVIOUS OVER IWAMI IN VIEW OF KIM

A. Proposed Combination and Motivation to Combine

A POSITA would have found it obvious, and would have been capable of modifying and motivated to modify, Iwami’s communication system 700 (“system 700”), and individual elements thereof and/or actions performed by those elements, by Kim’s teachings and/or the knowledge of a POSITA. A POSITA would have found it obvious and been motivated to configure Iwami’s control device 740 to transmit message-based commands of the type taught by Kim to Iwami’s information processing device 730 (“sink device 730”)/display device 731 and to Iwami’s information processing devices 710, 720 (“source devices 710, 720”) for controlling connections to, and controlling display operations on, Iwami’s sink device 730/display device 731 (as discussed in detail below) for several reasons.

EX1003, ¶55

For example, both references are analogous art from the same field of endeavor and are reasonably pertinent to the some of the particular problems to which Iwami and Kim are directed, including problems relating to media transmission and display in a network environment. EX1004, (57), [0002], [0009]; EX1005, [Abstract], [0001], [0008]; EX1006 (57), [0001], [0018]; EX1007, [0007], [0020]-[0028]. Specifically, the second embodiment of Iwami is a system 700 where source devices 703, 704, 710, and/or 720 can send image data to sink device 730 connected to a display device 731 that displays the image data. A control device 740 manages connections between source devices 703, 704, 710, and/or 720 and sink device 730. EX1004, [0235]-[0256]; EX1005, [0186]-[0207]. Similarly, Kim describes a multicast streaming service where a media server 120 sends media data to one or more media renderers 131-136 that display the media data. A control point 110 manages connections between the media server 120 and media renderers 131-136. EX1006, [0035]-[0047]; EX1007, [0041]-[0054]; EX1003, ¶55.

Iwami generally teaches that the connections between source devices 703, 704, 710, and/or 720 and sink device 730 are formed, maintained, and/or terminated according to permission from control device 740. EX1004, [0406]-[0407], [0448]-[0455]; EX1005, [0330]-[0331], [0372]-[0377]. Kim describes specific systems, messages, and signal sequences by which the control point 110

can grant and/or revoke permission for connections between the media server 120 sends media data to one or more media renderers 131-136. EX1006, [0037]-[0045]; EX1007, [0043]-[0052]; EX1003, ¶56.

Iwami demonstrates the desirability of permission for connection control, but arguably does not clearly describe a technical process for permissions-based connection management. A POSITA would have been motivated to implement elements of the Kim permission technique as one mechanism by which the control device 740 of Iwami can manage connections between source devices 703, 704, 710, and/or 720 and sink device 730. This would have simply involved combining known prior art elements (the system 700 elements of Iwami) according to known methods (the messaging described by Kim) to yield predictable results (a system 700 whose elements can communicate with one another, or not, based on permission or lack thereof). A POSITA would have understood that there would have been a reasonable expectation of success in doing so, because Kim supplies a complete description of a technique for granting and revoking connection permission that is compatible with the system 700 of Iwami, and because implementing Kim's message-based techniques in Iwami's system would involve only ordinary skill. EX1003, ¶57

Iwami teaches transmitting and receiving commands to remotely control display operations. For example, control device 740 sends information to sink

device 730 that causes sink device 730 to change the size and/or position of images from source devices 703, 704, 710, and/or 720. EX1004, [0296]-[0308]; EX1005, [0247]-[0356]. Similarly, Kim teaches a control point 110 sending commands to start and/or stop video play and/or transmission. EX1006, [0040]-[0044]; EX1007, [0046]-[0051]; EX1003, ¶57, 68, 69, 79, 82.

Because Iwami and Kim both describe examples of commands to remotely control display operations, with Kim teaching specific messages that can include commands, a POSITA would have been motivated to include commands and/or messaging of the type discussed by Kim as one mechanism by which the control device 740 of Iwami can control display operations of sink device 730. This would have simply involved combining known prior art elements (i.e., the system 700 elements of Iwami) according to known methods (i.e., the messaging described by Kim) to yield predictable results (i.e., a system 700 with a control device 740 that can control operations of other devices, such as sink device 730, by transmitting commands). A POSITA would have understood that there would have been a reasonable expectation of success in doing so, because Kim describes examples of display operation commands and messages compatible with the system 700 of Iwami. EX1003, ¶57

B. Claim 1

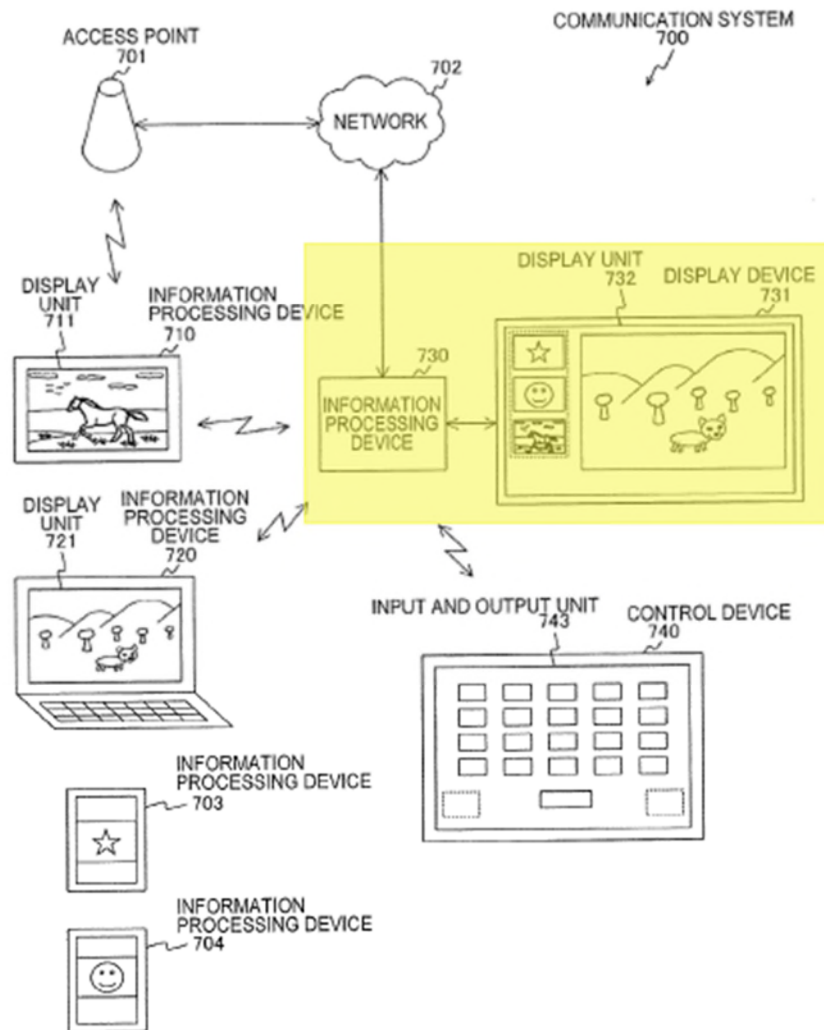
1. [1pre]

To the extent the preamble is limiting, Iwami and Kim each disclose a communication system. Iwami describes a system 700 in a second embodiment that includes an access point 701, a network 702, information processing devices 703, 704, 710, 720, 730, a display device 731, and a control device 740. EX1004, FIG. 17, [0235]-[0236]; EX1005, FIG. 17, [0186]-[0187]. Kim discloses a multicast streaming service method and system wherein a control point 110, media server 120, and media renderers 131-136 communicate with one another. EX1006, FIG. 1, [0018], [0032]-[0036]; EX1007, FIG. 1, [0021]-[0028], [0038]-[0041]; EX1003, ¶58-60.

2. [1a]

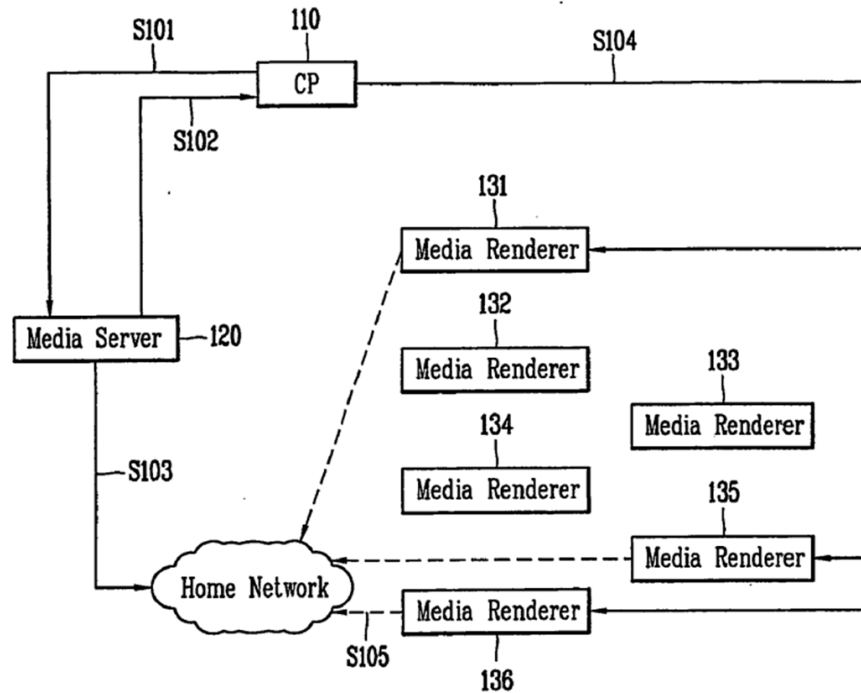
Iwami and Kim each disclose a communication device. In Iwami's system 700, the combination of sink device 730 and display device 731 (which includes a display unit 732 and which can be included in or coupled via a wired or wireless connection to sink device 730), is a claimed communication device. The sink device 730 has a display function for displaying information on a screen of a television or projector. The sink device 730 displays an image on display device 731. EX1004, FIG. 17, [0248]-[0249]; EX1005, FIG. 17, [0199]-[0200]; EX1003, ¶61-62.

FIG. 17



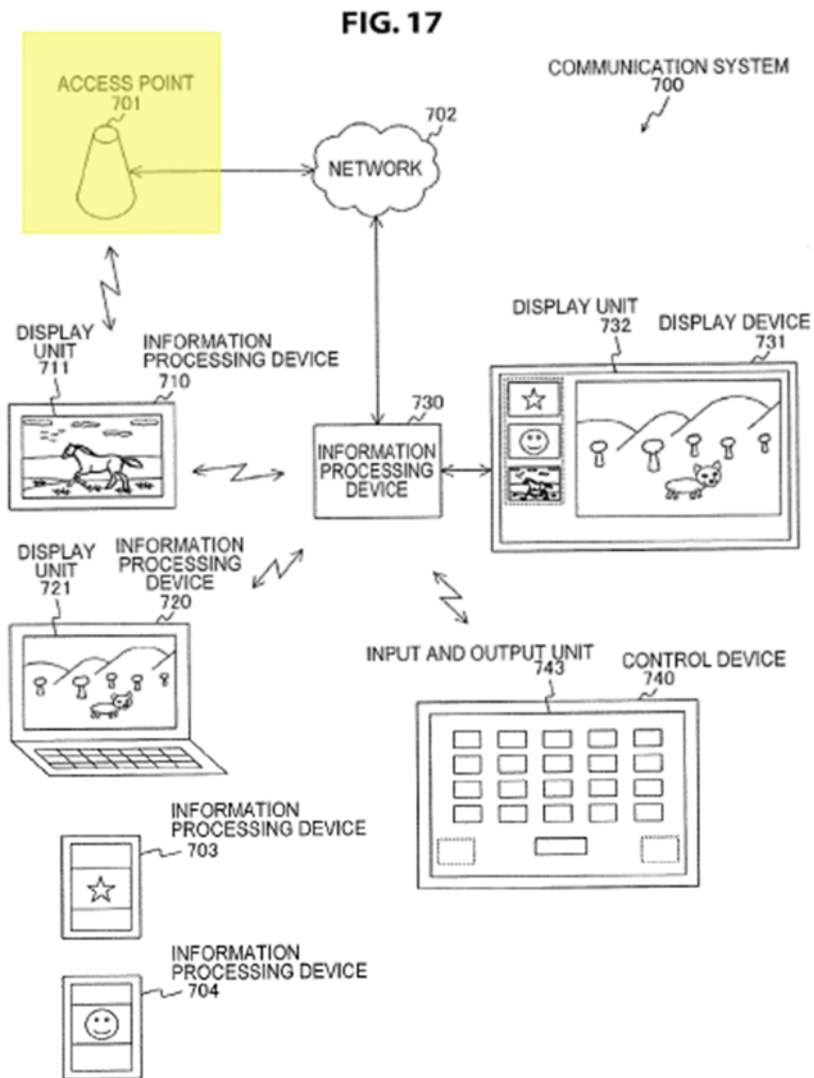
In Kim's system, media renderers 131-136 are communication devices. For example, Kim discloses that one of the media renderers 131-136 requests to join a multicast group and, once joined, plays contents sent from media server 120, thereby allowing a user to watch the contents. EX1006, [0042]-[0044]; EX1007, [0048]-[0051]; EX1003, ¶63.

FIG. 1



3. [1b]

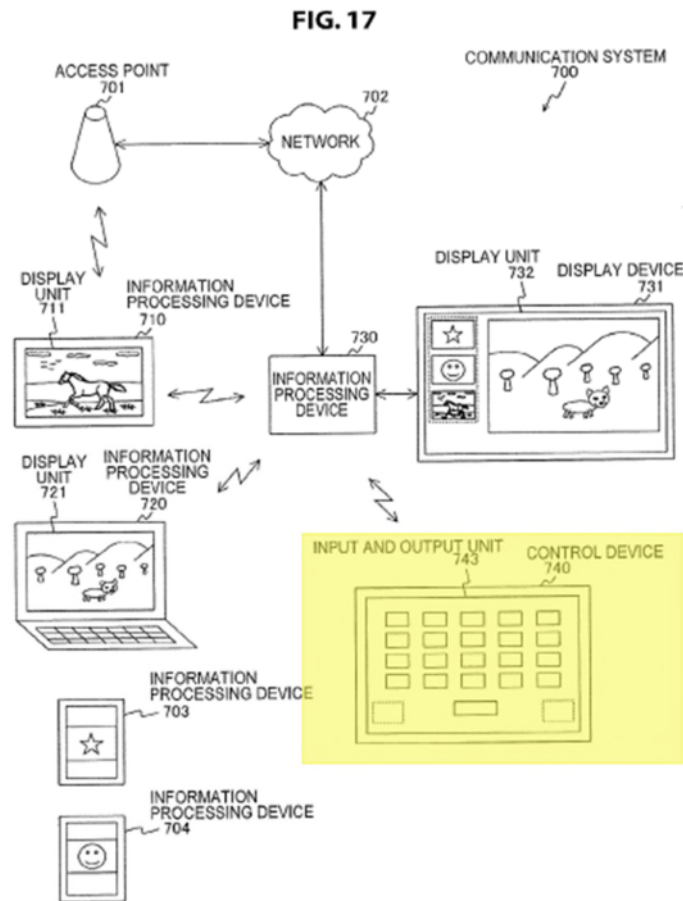
Iwami discloses an access point device. For example, the system 700 of Iwami includes access point 701, which is a wireless LAN (e.g., WiFi) access point. Access point 701 is connected to sink device 730 by a wired or wireless connection. EX1004, [0238]; EX1005, [0189]. Source devices 703, 704, 710, and 720 also connect to access point 701. Control device 740 also connects to the access point 701 and thereby communicates with other devices via access point 701. EX1004, FIG. 17, [0237]-[0239], [0250]; EX1005, FIG. 17, [0188]-[0190], [0201]; EX1003, ¶64-65.



4. [1c]

Iwami discloses this limitation, and to the extent that Iwami does not disclose it, the combination of Iwami and Kim render it obvious. In Iwami's system 700, control device 740 is the claimed first communication terminal. In one embodiment, control device 740 connects to sink device 730/display device 731

via access point 701 (not shown in Fig. 17). EX1004, [0250]; EX1005, [0201];
EX1003, ¶66-67.

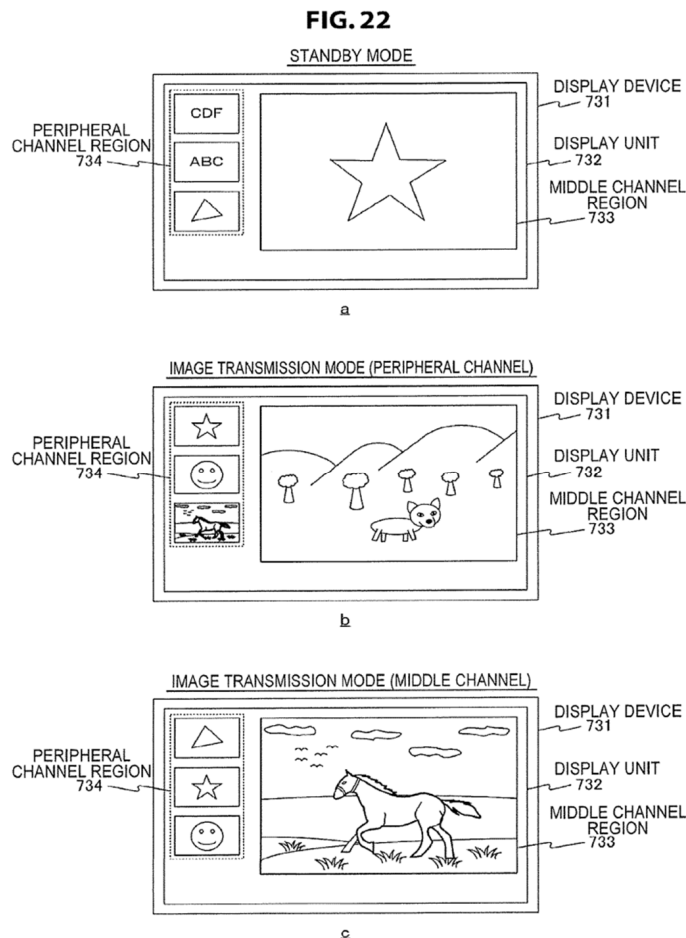


Control device 740 transmits commands to remotely control display of information on sink device 730/display device 731 (the claimed “communication device”). Specifically, Iwami describes an example in which students give presentations in a classroom using source devices 703-705 and 720 (each a “second communication terminal” as discussed below). A student can give a presentation while causing an image related to the presentation to be displayed on display device 731. By manipulating control device 740, a teacher can sequentially

select the source devices of the students and thereby cause, via a command sent to the sink device 730 as discussed in EX1004, [0304], the image of the selected information processing device to be displayed on display unit 732 of display device 731 in a peripheral channel region 734 and subsequently (e.g., via selection of other students' source devices) cause the image of that source device to be moved to the middle channel region 733. EX1004, [0252]-[0255], [0291], [0304] and Figs. 17, 18 and 21; EX1005, [0203]-[0206], [0242], [0255] and Figs. 17, 18 and 21; EX1003, ¶68.

For example, with reference to Fig. 22b below, three source devices are transmitting video corresponding to a star, smiley face and horse to the sink device 730 in a low frequency band, and those video images are displayed in the upper, center and lower part of the peripheral channel region 734. At the same time, a fourth source device is transmitting video corresponding to a small animal which is displayed in the middle channel region 733. In response to a teacher at control device 740 selecting a new source device, the control device sends a command to the sink device 730 that results in the new source device being commanded by the sink device 730 to transition from a standby mode and start transmitting triangle video information in a low frequency band, which is displayed in the upper part of peripheral channel region 733 as shown in Fig. 22c. The star and smiley face videos, which continue to be transmitted in the low frequency band, are moved to

the center and lower parts of the peripheral channel region, and source device transmitting the horse video is instructed by sink device 730 to transmit that horse video in the high frequency band, and the horse video is moved to the middle channel region 733 as shown in Fig. 22c. EX1004, [0284]-[0308]; EX1005, [0235]-[0256]; EX1003, ¶69.



Controlling by control device 740 the display device 731/display unit 732 to move a video display from peripheral channel region 734 to the middle channel region 733 is remotely controlling a display operation as recited in claim 1. As discussed below, to the extent that Iwami does not expressly disclose sending a

command from control device 740 to sink device 730, selection of a source device to be displayed on a display unit 732 of display device 731 using the interface of control device 740 triggers control device 740 to send a command to sink device 730/display device 731 in Iwami's system as modified by Kim's teachings.

EX1003, ¶70

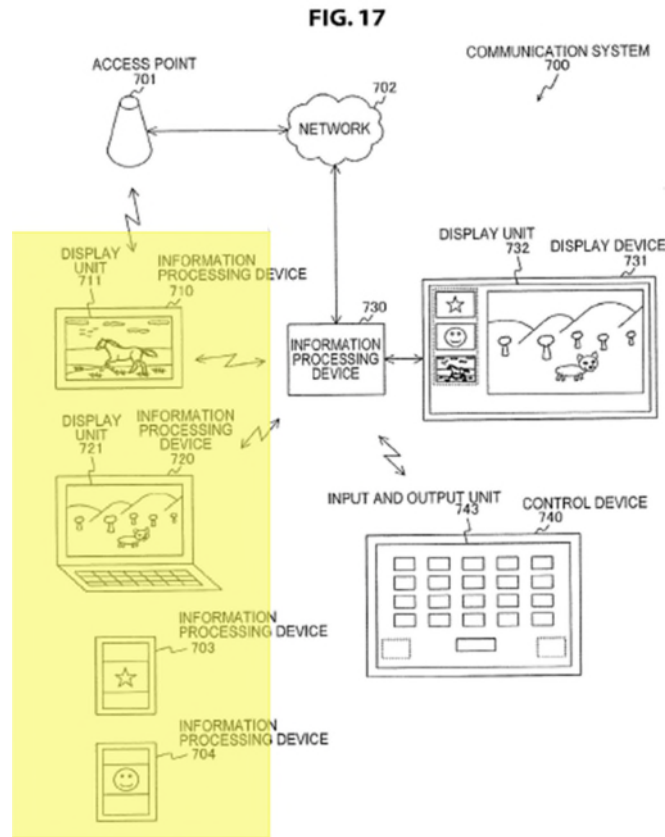
In Kim's system, control point 110 is a first communication terminal. For example, Kim discloses that control point 110 controls a media server and media renderer. This control includes invoking a MulticastStart() action that triggers one or more media renderers 131-136 to play the contents of data sent by media server 120. Invoking the MulticastStart() action causes media server 120 to respond with connection parameters and begin streaming, meaning that the MulticastStart() action functions as a command message sent by control point 110. EX1006, [0040]-[0044]; EX1007, [0046]-[0051]; EX1003, ¶71.

To the extent Iwami does not explicitly state that control device 740 sends a command in response to the teacher manipulating it to select a source device whose images will be displayed on display unit 732 of display device 731, Kim provides an example of how to send a command. A POSITA would have understood that the user input into control device 740 configures connections between source devices and/or display operation control on display device 731. A POSITA would have found it obvious to modify system 700 of Iwami to transmit a

command from a first communication terminal to remotely control a display operation on the communication device connected with the first communication terminal. In other words, a POSITA would have found it obvious to configure control device 740 to send a command to either source device 710, sink device 730, or both, as taught by Kim when Kim describes sending a MulticastStart() action message. A POSITA would not need to use the specific MulticastStart() action message of Kim, but rather would have understood that a message including a command can be transmitted. As discussed above, a POSITA would have been motivated to combine Iwami and Kim because they are in a same field of art, Iwami teaches that providing remote control of display operations is desirable, and Kim describes a known technique for sending control commands that a POSITA would reasonably have expected to be successful. EX1003, ¶72

5. [1d]

Iwami discloses this limitation, and to the extent not disclosed by Iwami, the combination of Iwami and Kim renders it obvious. In Iwami's system 700, source devices 703, 704, 710, and 720 are the claimed second communication terminals. EX1004, [0240], [0246]; EX1005, [0191], [0197]; EX1003, ¶73-74.



As discussed above in limitation [1c], Iwami alone or in combination with Kim teaches that by manipulating control device 740 (the first communication terminal), a teacher can sequentially select the source devices of the students (e.g., source devices 703, 704, 710, and 720) and thereby cause the image of the selected source device to be displayed on a display unit 732 of display device 731 (initially in the peripheral channel region 734 and then in the middle channel region 733 as discussed at [0291]-[0295]). As such, the first communication terminal enables the second communication terminal (the student's source device) to use sink device 730/display device 731 to display video. When the user of control device 740

selects a source device 710, or 720, control device 740 “performs control such that the communication mode is set in the source device (selected information processing device 710, or 720) based on the manipulation input.” EX1004, [0252]-[0255], [0264]; EX1005, [0203]-[0206], [0215]; EX1003, ¶75.

Iwami also teaches that connections between the second communication terminals (e.g., device 710) and the communication device (i.e., device 730) rely on permissions. When source device 710 is connecting to sink device 730 so it can send video information to sink device 730, source device 710 determines whether or not connection permission information has been received from device 730 (as discussed above, the connection permission information originates with control device 740). When connection permission information has been received, device 710 and device 730 complete remaining steps to establish a connection with one another. Iwami teaches that connection information permission or non-permission can be set each time there is a connection request from the source device (i.e., each time control unit 740 sets the communication mode of the source device as discussed above). EX1004, [0409], [0413], [0448]-[0455]; EX1005, [0333], [0337], [0372]-[0377]; EX1003, ¶76.

Iwami also teaches that the permission can originate with the first communication terminal (i.e., control device 740), and is therefore “from” the first communication terminal. For example, Iwami describes a situation where source

device 710 is trying to connect with sink device 730 by a connection other than that provided by access point 701, referred to as “outdoor use” in Iwami. In this example, control device 740 supplies “outdoor use” permission to sink device 730. When source device 710 sends a connection request to sink device 730, sink device 730 responds with connection permission information including outdoor use permission received from control device 740. Specifically, Iwami states that “when the information processing device 730 transmits the connection permission information in response to the connection request received via the access point 701 (AP), the information processing device acquires the outdoor use information (permission or non-permission) from the control device 740, includes the acquired outdoor use information (permission or non-permission) in the connection permission information, and transmits the resulting connection permission information.” EX1004, [0407]; *see also* [0405]-[0407]; EX1005, [0331]; *see also* [0329]-[0331]; EX1003, ¶77.

Because the outdoor use permission is included in the connection permission information used by source device 710 (second communication terminal) to connect to sink device 730 (communication device), the outdoor use permission is a part of the permission to establish a connection with the communication device to use the communication device. Because the outdoor use permission comes from control device 740 (first communication terminal) and is included in the

connection permission information sent from device 730 to device 710, the second communication terminal has received permission from the first communication terminal 740 when the second communication terminal receives the connection permission information, notwithstanding that the connection permission information passes through sink device 730. EX1003, ¶78

To the extent Iwami's outdoor use permission is not unambiguously permission from the first communication terminal such that if the second communication terminal has the permission, it establishes a connection with the communication device to use the communication device, a POSITA would have found it obvious to send all connection permission information (not only outdoor use permission) from control device 740 to sink device 730. Iwami teaches that a user of control device 740 uses the touch screen to select the outdoor use permission that is sent from control device 740 to sink device 730. EX1004, [0410], EX1005, [0334]; EX1003, ¶79.

To the extent this feature is not explicit in Iwami, a POSITA would have found it obvious to modify control device 740 to also accept user input of connection permission generally, meaning that any and all connection permission information would originate with control device 740 and be passed to source device 710 via sink device 730. A POSITA would have been motivated to include this feature both as a natural extension of the outdoor use permission already

described explicitly and as a consequence of the fact that Iwami explicitly teaches that control device 740 performs group management generally, and membership in a group specified by control device 740 is used as a basis for granting permission to connect to sink device 730. See EX1004, [0266]-[0273], [0357]-[0362]; EX1005, [0217]-[0224], [0281]-[0286]. Thus, a POSITA would have found it obvious to configure control device 740 to send permission information stored by control device 740 (e.g., group membership and/or outdoor use permission) to sink device 730, and in turn, to configure sink device 730 to send this permission information to source device 710 as already taught by Iwami. EX1003, ¶79

6. [1e]

Iwami discloses this limitation, and to the extent not disclosed by Iwami, the combination of Iwami and Kim renders it obvious. EX1003, ¶80

In Iwami's system 700, control device 740 operates as a first communication terminal, connecting to sink device 730/display device 731 via access point 701 and transmitting commands to control display of information on sink device 730/display device 731. As noted above for limitation [1c], Iwami describes that a teacher using control device 740 can sequentially select students' devices (e.g., 710, 720) and thereby cause control device 740 to transmit a command to sink device 730 that causes the image of the selected source device to be displayed in a selected region. See limitation [1c] above. EX1003, ¶81.

Causing the image from the selected source device to be moved from the peripheral channel region 734 to the middle channel region 733 constitutes controlling how to display the data received from the second communication terminal by the communication device in accordance with a command received from the first communication device while the communication device outputs data received from the second communication terminal while maintaining the connection with the second communication terminal as required by limitation [1e]. EX1003, ¶82-83

In Kim's system, control point 110 is a first communication terminal. As discussed above, Kim discloses that control point 110 controls a media server and media renderer by invoking a MulticastStart() action that triggers one or more of media renderers 131-136 to play the contents of data sent by media server 120. EX1006, [0040]-[0044]; EX1007, [0046]-[0051]. A POSITA would have found it obvious to implement the commands from Iwami's control device 740 discussed above using a message like the MulticastStart() action message disclosed by Kim for the reasons discussed above for limitation [1c]. EX1003, ¶84

7. [1f]

Iwami discloses that when a student information processing device enters the standby mode (e.g., when a student's video is removed from the middle channel region 733 in response to a command from control device 740 to the

display device as discussed above), a connection between source device 710 and sink device 730 is terminated. EX1004, [0374]; EX1005, [0325]. This command from control device 740 to sink device 730 constitutes information to terminate the permission of the second communication device to directly connect to sink device 730. Iwami further discloses that control device 740 manages source device 710. EX1004, [0283]; EX1005, [0234]; EX1003, ¶85.

Iwami also teaches that there can be conditions wherein permission is not granted to a user, such as “in a time zone in which a presentation or a conference that is highly confidential, a presentation or a conference that has a high degree of importance, a meeting that has not to be exposed, or the like is performed.” EX1004, [0273]; EX1005, [0224]; EX1003, ¶86.

However, Iwami does not disclose a mechanism by which control device 740 terminates the permission of source device 710 to connect to sink device 730. Given the teaching in Iwami that it may be necessary or desirable to withhold permissions from certain users during certain times, a POSITA would have found it obvious to provide the capability to terminate previously granted permission in a case where it later becomes necessary or desirable to do so. A POSITA would have looked to other prior art to implement this functionality. EX1003, ¶87

Kim discloses a communication device receiving information to terminate permission from a first communication terminal and the communication device

terminating the connection in accordance with the information to terminate permission received from the first communication terminal. EX1003, ¶88

In Kim, after the MulticastStart() action is invoked and media server 120 (second communication terminal) is sending content to at least one of the media renderers 131-136 (communication device), control point 110 (first communication terminal) can invoke a Leave() action to at least one of media renderers 131-136. The Leave() action is information to terminate the permission, sent from the first communication terminal to the communication device, that configures the communication device to terminate the connection with the second communication terminal in accordance with the Leave() command. That is, upon receiving a Leave() command, a media renderer 131-136 will stop receiving data from media server 120. Indeed, Kim teaches that media renderer 131-136 will “stop the data reception,” indicating that the connection is terminated. EX1006, [0037], [0045]-[0046]; EX1007, [0043], [0052]-[0053]; EX1003, ¶89.

Based on Kim’s teachings, a POSITA would have found it obvious to modify the system 700 of Iwami to send an explicit message from first communication terminal 740 to sink device 730 to terminate permission for a second communication terminal 710 to connect with sink device 730. In other words, a POSITA would have found it obvious for the reasons discussed above to configure control device 740 to send a message as taught by Kim to sink device

730 indicating that permission for source device 710 to connect to sink device 730 has been revoked. A POSITA would have understood that it was not necessary to use the specific Leave() action message of Kim, but rather would have understood that any suitable message could be used to terminate the permission. As discussed above, a POSITA would have been motivated to combine Iwami and Kim because they are in a same field of art, Iwami teaches that terminating permission is desirable, and Kim describes a known technique for terminating such permission that a POSITA would reasonably expect to be successful. EX1003, ¶90

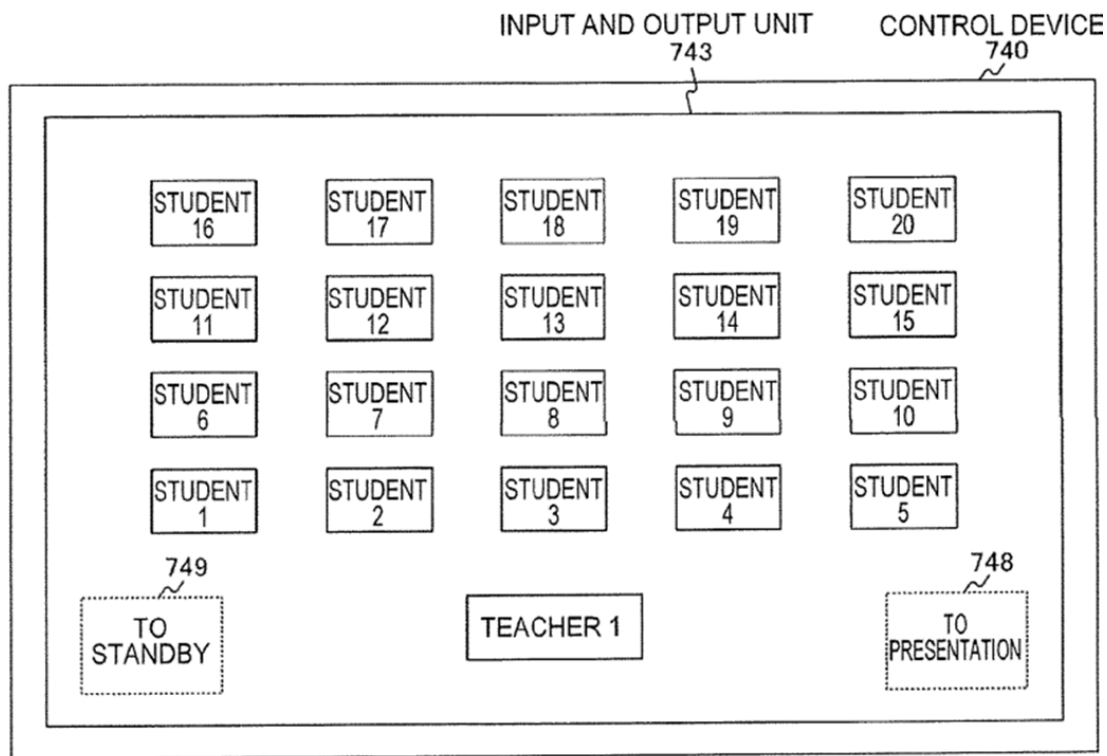
C. Claim 5

1. [5a]

Iwami and Kim render claim 1 obvious. Iwami discloses this limitation and, to the extent not disclosed in Iwami, the combination of Iwami and Kim renders it obvious. For example, Iwami teaches that a teacher can select source devices (second communication terminals) to send information to sink device 730/display device 731 (communication device) by manipulating control device 740 (first communication terminal) as discussed for limitation [1c]. Control device 740 includes a touch screen that shows information and accepts user inputs. The touch screen shows students 1-20, a presentation region 748, and a standby region 749. The presentation region 748 is used to switch from standby mode to image transmission mode (i.e., putting a student 1-20 in the presentation region connects

their device with the communication device) and, as discussed for limitation [1c], will cause a student source information processing device currently in the middle channel image transmission mode to be placed into standby. The standby region 749 is also used to switch from image transmission mode to standby mode. In standby mode, the direct connection between the student device and sink device 730 is disconnected, which terminates the student device's ability to send images to display device 731 (i.e., moving a student 1-20 from the presentation region to the standby region disconnects a direct connection between their device and the communication device and thereby terminates permission to send images through the direct connection). EX1004, [0374]; EX1005, [0325]. The teacher can select icons of students 1-20 to move them into the presentation region 748 and/or the standby region 749. EX1004, FIG. 21, [0255], [0261]-[0263], [0274]-[0276], [0281]-[0282], [0302]-[0307]; EX1005, [0206], [0212]-[0214], [0225]-[0227], [0232]-[0233], [0250]-[0255]; EX1003, ¶91.

FIG. 21



As discussed above, to the extent the action taking place in Iwami is not explicitly described as terminating permission, Kim describes that the information terminating connection is information to terminate permission. See [1f]. EX1003, ¶192

2. [5b]

Iwami discloses this limitation and, to the extent not disclosed in Iwami, the combination of Iwami and Kim render it obvious. Iwami teaches receiving an input operation for terminating the permission and transmitting the information to terminate the permission to the communication device. As noted above, the touch

screen of control device 740 lets the teacher switch a student device from standby mode to image transmission mode (i.e., putting a student 1-20 in the presentation region connects their device with the communication device) and, as discussed above, will cause another student's device currently in the main channel transmission mode to be switched into the standby mode. See limitation [5a]. Pressing the standby region 749 is used to switch from image transmission mode to standby mode. Both actions are input operations. In both cases, moving a student 1-20 from the presentation region to the standby region disconnects their device from communication device/sink device 730. The teacher can select icons of students 1-20 to move them into the presentation region 748 and/or the standby region 749. When the teacher moves an icon from the presentation region 748 to the standby region 749, the corresponding student information processing device is switched to the standby mode and no longer connects to sink device 730 to send display information to sink device 730. When this happens, control device 740 (first communication terminal) outputs notification information to sink device 730 (communication device) indicating that the communication mode of the student's device (second communication terminal) has changed (e.g., to standby mode). In the standby mode, the student device (e.g., device 710) disconnects a direct connection with sink device 730. EX1004, FIG. 21, [0255], [0261]-[0263], [0274]-

[0276]. [0281]-[0282], [0302]-[0307], [0389]-[0390]; EX1005, [0206], [0212]-[0214], [0225]-[0227], [0232]-[0233], [0250]-[0255], [0313]-[0314]; EX1003, ¶93.

As discussed above, to the extent the information of Iwami is not explicitly described as relating to permission, Kim describes that the information terminating connection is information to terminate permission. See limitation [1f]. EX1003, ¶94

As described at limitation [1f], a POSITA would have found it obvious to modify the system 700 of Iwami to send an explicit message from a first communication terminal to terminate permission for a second communication terminal to connect with a communication device as taught by Kim. EX1003, ¶95

D. Claim 13

1. [13a]

Iwami and Kim render claim 1 obvious. Iwami discloses this limitation and, to the extent not disclosed in Iwami, the combination of Iwami and Kim render it obvious. As discussed in section [1e], Iwami teaches that in cases such as those illustrated in FIG. 22b and 22c, the connection between source device 710 and sink device 730 is maintained as the image transmission mode changes from the low frequency band in FIG. 22b to the high frequency band in FIG. 22c. That is, the image is transmitted from source device 710 to sink device 730 and displayed in the peripheral channel region 734 in FIG. 22b and, when a command comes from

control device 740 to switch the mode as described above, the image continues to be transmitted from source device 710 to sink device 730 but is now displayed in the middle channel region 733 in FIG. 22c. EX1004, [0284]-[0295]; EX1005, [0235]-[0246]. During the period of this transition, sink device 730 is being controlled by second communication terminal/source device 710 in that this device is sending the data that is displayed by sink device 730 (initially in peripheral channel region 734 and later in middle channel region 733). EX1003, ¶96

Iwami also teaches that the command to switch the mode can come not only from control device 740, but also from a command entered into and transmitted from the source device in operation (B1). In such a case, the second communication terminal (source device such as source device 710) controls the communication device (sink device 730) while maintaining the connection with the communication device. EX1004, [0296]-[0302]; EX1005, [0247]-[0350]; EX1003, ¶97.

2. [13b]

Iwami discloses this limitation and, to the extent not disclosed in Iwami, the combination of Iwami and Kim render it obvious. As discussed for limitations [1c], [1e], and [13a], Iwami alone or as modified by Kim teaches control device 740 switching the mode used by sink device 730 by transmitting information (a command) to sink device 730 that causes the band of source device 710 to be

increased or decreased. During the period of this transition, sink device 730 is also being controlled by control device 740 in that this device is sending information that determines where sink device 730 will display the information from source device 710. The information is transmitted from control device 740 to sink device 730, indicating that the connection between the two is maintained. Moreover, as described above, control device 740 can connect to access point 701 and communicate with sink device 730 via access point 701. EX1004, [0250]. [0296]-[0308]; EX1005, [0247]-[0356]; EX1003, ¶98; see also limitation [1b].

E. Claim 14

1. [14pre]

Iwami in view of Kim teaches a communication terminal. See 1(pre) and 1(c) (e.g., first communication terminal of claim 1). EX1003, ¶99

2. [14a]

See [1a], [1b], and [1c] (e.g., where the first communication terminal of claim 1, Iwami's control device 740, is configured to connect to the communication device of claim 1, Iwami's sink device 730, via the access point device of claim 1, Iwami's access point 701). In one embodiment, control device 740 connects to sink device 730 via access point 701 (not shown in Fig. 17). EX1004, [0250]; EX1005, [0201]. Iwami's control device 740 has a wireless connection interface configured to connect to a communication device (sink device

730) via an access point device (access point 701) in this embodiment. EX1003,

¶100

3. [14b]

See [1a] and [1c] above. EX1003, ¶101

4. [14c]

See [1c] and [1d] above. EX1003, ¶102

5. [14d]

See [1e] above. EX1003, ¶103

6. [14e]

See [1f] above. EX1003, ¶104

F. Claim 15

1. [15pre]

See [1pre] and [1a] (e.g., communication device of claim 1, Iwami's sink device 730/display device 731). EX1003, ¶105

2. [15a]

Iwami in view of Kim teaches a wireless connection interface configured to connect to a communication terminal and another communication terminal. See [1a], [1b], [1c], [1d] and [14a] (e.g., where the first communication terminal of claim 1, Iwami's control device 740, connects to the communication device of claim 1, Iwami's sink device 730, via the access point device of claim 1, Iwami's access point 701, and the second communication terminal of claim 1, an Iwami

student device 710 or 720, connects to the communication device). Iwami's sink device 730/display device 731 includes a wireless communication unit 320 which is configured to connect to a control device 740 and an Iwami student device 710 or 720. EX1004, [0103]; EX1005, [0054]. EX1003, ¶106

3. [15b]

See [1a] and [15a]; see also EX1004, [0103]; EX1005, [0054] (discussing control of wireless communication unit 320 by control unit 370, the claimed “controller”). EX1003, ¶107

4. [15c]

See [1a], [1b], and [1c]. EX1003, ¶108

5. [15d]

See 1[c] and 1[d] (e.g., where the second communication terminal of claim 1, an Iwami student device 710 or 720, establishes a connection with the communication device of claim 1, Iwami's sink device 730, if the first communication terminal of claim 1, Iwami's control unit 740, gives permission). EX1003, ¶109

6. [15e]

See [1e] (e.g., where the first communication terminal of claim 1, Iwami's control unit 740, transmits a command to control how to display data to the communication device of claim 1, Iwami's sink device 730, while the second communication terminal of claim 1, an Iwami student device 710 or 720, is

connected to the communication device and the communication device outputs data from the second communication terminal). EX1003, ¶110

7. [15f]

See [1f] (e.g., where the first communication terminal of claim 1, Iwami's control unit 740, transmits information to the communication device of claim 1, Iwami's sink device 730, to terminate the connection between the communication device and the second communication terminal of claim 1, an Iwami student device 710 or 720, and the communication device terminates the connection with the second communication terminal). EX1003, ¶111

VII. GROUND 2: CLAIMS 2 AND 12 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY

A. Proposed Combination and Motivation to Combine

Iwami, alone or as modified by Kim, teaches that devices can request to connect to other devices in a network, and such connections are allowed or terminated based on permissions. EX1004, [0318]-[0322], [0406]-[0407], [0448]-[0455]; EX1005, [0266]-[0270], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]. A POSITA would have found it obvious, and would have been motivated to, modify the Iwami-Kim system by incorporating elements of Liansky's security techniques, such as short range communication and/or scannable codes, to provide connection security within the system 700 of Iwami. Doing so would have simply involved

combining known prior art elements (i.e., the system 700 elements of Iwami, alone or in view of Kim) according to known methods (i.e., the security features of Liansky) to yield predictable results (i.e., a system 700 whose elements can communicate with one another, or not, based on permission or lack thereof with short range communication and/or scannable code features to enhance security).

EX1003, ¶112

Iwami, Kim, and Liansky are analogous art and are directed toward the same or similar problems. For example, as noted above, Iwami and Kim both relate to media transmission and display in a network environment and both discuss using permission to control connections between devices in the network environment. EX1004, (57), [0002], [0009], [0406]-[0407], [0448]-[0455]; EX1005, [Abstract], [0001], [0008], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]. Similarly, Liansky is directed to network communication, including security techniques such as transmitting a dynamic image code in a short-range communication by a first device and reading the code by a second device, and establishing a network connection using information encoded in the code. EX1012, (57), 1:32-49, 2:5-24. For example, Liansky describes a process where a QR code or other scannable code encodes connection information. Upon scanning this code at short range, a

device can decode the connection information and use it to connect to a network device. EX1012, 5:3-37; EX1003, ¶113.

A POSITA would have been capable of modifying, and motivated to modify, Iwami's system 700 (considered alone or as modified by Kim and/or a POSITA's knowledge), and individual elements thereof and/or actions performed by those elements, by Liansky's teachings and would have understood that Liansky supplies a complete description of security features that are compatible with the system 700 of Iwami. EX1003, ¶114

B. Claim 2

1. [2pre], [2a]

As discussed with respect to limitation [1d], Iwami discloses or renders obvious a first communication terminal giving permission to a second communication terminal to connect with a communication device. Liansky teaches sending connection information using a form of short-range communication, specifically displaying a bar code representing connection information on a display screen of a first device, wherein a second device captures an image of the bar code with a camera to read the connection information. (In this regard, short-range communication is defined in claim 12 to include this form of communication (displaying a bar code by one device and capturing an image of the bar code by a second device), which is also consistent with the description of short-range

communication in EX1001 at 4:67-5:1 and 26:7-17). For example, Liansky teaches that a barcode is an optical machine-readable representation of data relating to the object to which it is attached, and gives a QR-code as a specific example of a two-dimensional barcode. EX1012, 3:35-37, 4:4-8; EX1003, ¶115.

In FIG. 2, Liansky illustrates a process of connecting mobile wireless device 120 and screen device 110 for video streaming from mobile wireless device 120 to screen device 110. In this process, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). Mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37; EX1003, ¶116.

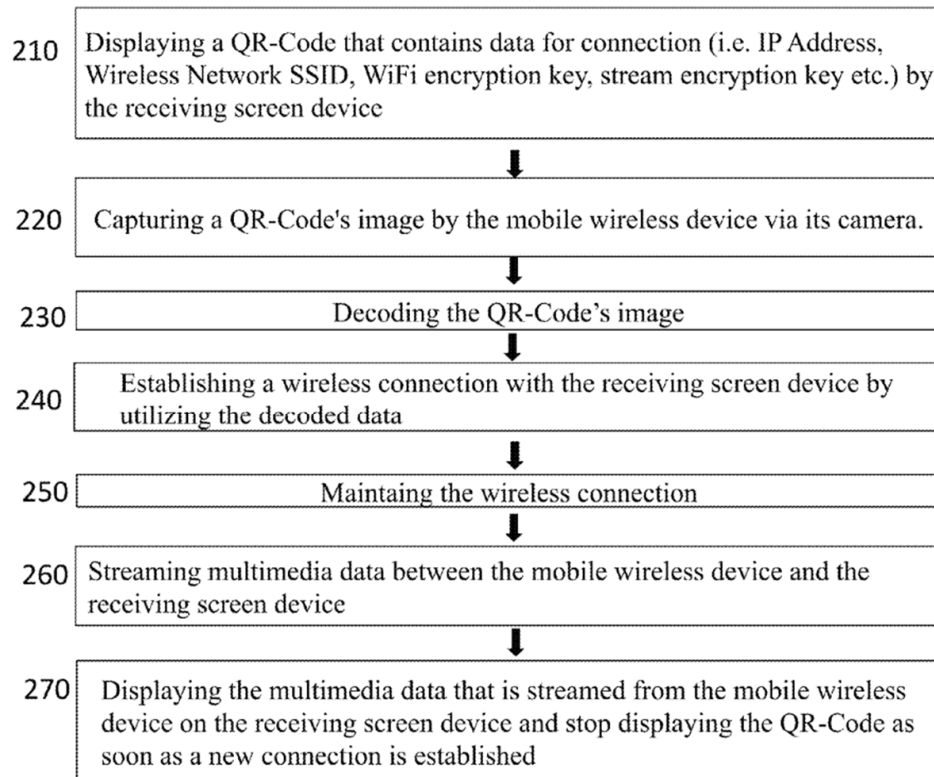


Fig.2

Based on Liansky's teachings, a POSITA would have modified the system 700 of Iwami, alone or in view of Kim, to configure any and/or all of the devices within system 700 to transmit bar codes representing connection information and/or any and/or all of the devices within system 700 to read the connection information from the bar codes. A POSITA would not necessarily send the exact sequence of messages to/from the exact sources/destinations specified by Liansky. Rather, a POSITA would have understood from Liansky that messages can include bar codes including connection information. As discussed above, a POSITA would have been motivated to combine the Iwami-Kim system with Liansky because they are in a same field of art, Iwami teaches that communicating permission and/or

connection information is desirable, and Liansky describes specific message content, including bar codes, that a POSITA would reasonably expect to be successful when used in combination with the Iwami-Kim system. EX1003, ¶117

C. Claim 12

1. [12a]

As discussed with respect to claims 1 and 2, Iwami in view of Kim and Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device, the permission includes connection information necessary for a connection, and the connection is through a short range communication. EX1003, ¶118

As discussed above, Liansky describes a process of connecting a mobile wireless device 120 and a screen device 110 for video streaming from the mobile wireless device 120 to the screen device 110 using transmission and receipt of a QR code (bar code) including connection information used to establish the connection.. See limitation [2a]. EX1012, FIG. 2, 5:3-37; EX1003, ¶119.

2. [12b]

As discussed with respect to claims 1 and 2, Iwami in view of Kim and Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device. In the Iwami-Kim-Liansky combination, the first communication terminal transmits connection information to the second communication terminal and the transmitting is through

a short-range communication from the first communication terminal to the second communication terminal. As discussed by Iwami, the second communication terminal connects to the communication device in response to receiving permission, and as discussed by Liansky, the connection is made by using the connection information provided in the QR code. EX1004, [0409], [0413], [0448]-[0455]; EX1005, [0333], [0337], [0372]-[0377]; EX1012, FIG. 2, 5:3-37; EX1003, ¶120. See 1(d), 2, and 12(a) above.

3. [12c]

As discussed above, Liansky teaches short-range communication wherein a display screen of a first device displays a bar code representing connection information, and a second device captures an image of the bar code with a camera to read the connection information. For example, Liansky teaches that a barcode is an optical machine-readable representation of data relating to the object to which it is attached, and gives a QR-code as a specific example of a two-dimensional barcode. EX1012, 3:35-37, 4:4-8; EX1003, ¶121. *See also* claim 2 above.

In FIG. 2, Liansky illustrates a process of connecting a mobile wireless device 120 and a screen device 110 for video streaming from the mobile wireless device 120 to the screen device 110. In this process, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection

information represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera, decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37; EX1003, ¶122.

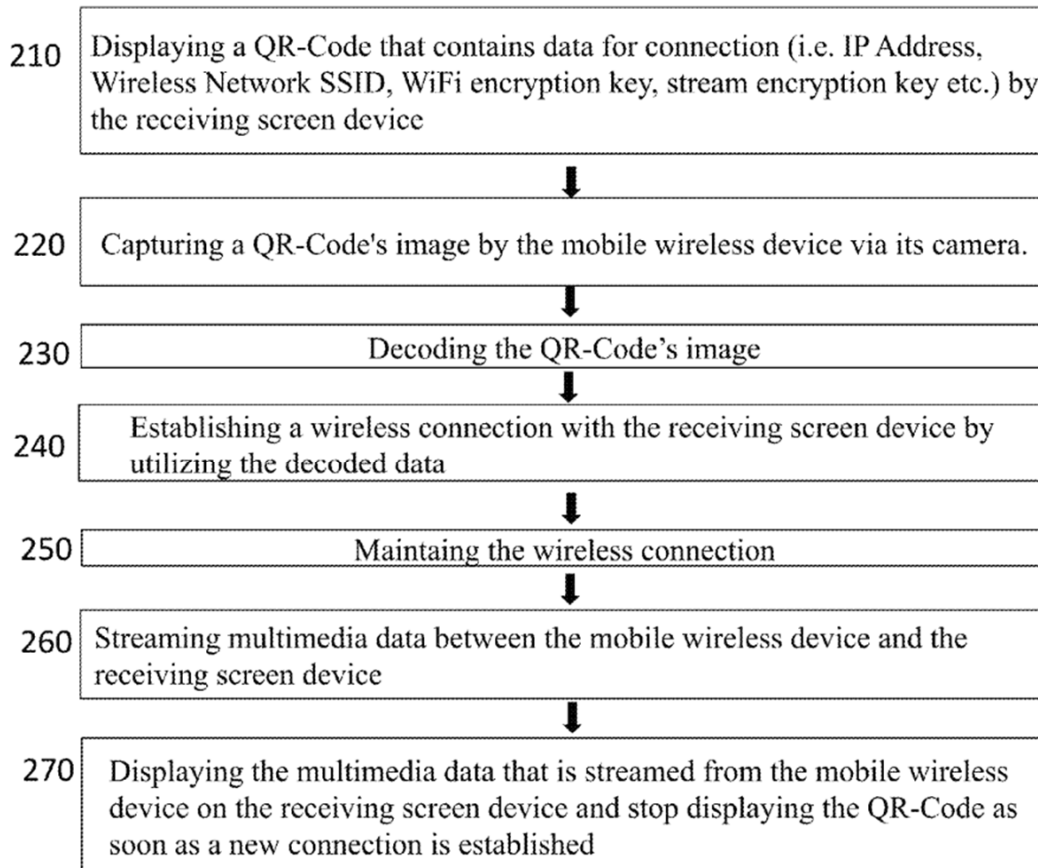


Fig.2

Based on Liansky's teachings, a POSITA would have modified the system 700 of Iwami, alone or in view of Kim, to configure any and/or all of the devices within system 700 to transmit bar codes representing connection information and/or any and/or all of the devices within system 700 to read the connection information from the bar codes. A POSITA would not necessarily send the exact

sequence of messages to/from the exact sources/destinations specified by Liansky.

Rather, a POSITA would have understood from Liansky that messages can include bar codes including connection information. As discussed above, a POSITA would have been motivated to combine the Iwami-Kim system with Liansky because they are in a same field of art, Iwami teaches that communicating permission and/or connection information is desirable, and Liansky describes specific message content, including bar codes, that a POSITA would reasonably expect to be successful when used in combination with the Iwami-Kim system. EX1003, ¶123

VIII. GROUND 3: CLAIMS 7, 8, AND 10 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY AND WEISER

A. Proposed Combination and Motivation to Combine

Iwami, alone or as modified by Kim, teaches that devices can request to connect to other devices in a network, and such connections are allowed or terminated based on permissions. EX1004, [0318]-[0322] , [0406]-[0407], [0448]-[0455]; EX1005, [0266]-[0270], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]. A POSITA would have found it obvious, and would have been motivated to, modify the Iwami-Kim-Liansky system by implementing elements of the Weiser permission and security techniques including the use of blacklists and/or whitelists to provide connection security and a straightforward way for control device 740 of Iwami to enable and/or disable connections by source devices 703, 704, 710,

and/or 720. Doing so would have simply involved combining known prior art elements (i.e., the system 700 elements of Iwami, alone or in view of Kim and Liansky) according to known methods (i.e., the security features of Weiser) to yield predictable results (i.e., a system 700 whose elements can communicate with one another, or not, based on permission or lack thereof with whitelist and blacklist features to enhance security and connection management). EX1003, ¶124

Iwami, Kim, Liansky and Weiser are analogous art and are directed toward the same or similar problems. For example, as noted above, Iwami and Kim both relate to media transmission and display in a network environment and both discuss using permission to control connections between devices in the network environment, and Liansky relates to additional permission and/or security controls for the connections in the same or similar network environment. EX1004, (57), [0002], [0009], [0406]-[0407], [0448]-[0455]; EX1005, [Abstract], [0001], [0008], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]; EX1012, (57), 1:32-49, 2:5-24. Similarly, Weiser is directed to streaming video content in a network environment. EX1008, (57), [0001], [0006]. Weiser also discloses the importance of security for the network environment, and in particular describes how connection permission can be managed using blacklists and whitelists. EX1008, [0185]-[0202]; EX1003, ¶125.

A POSITA would have been capable of modifying Iwami's system 700 (considered alone or as modified by Kim, Liansky, and/or a POSITA's knowledge), and individual elements thereof and/or actions performed by those elements, by Weiser's teachings, would have had a reasonable expectation of success in so doing, and would have understood that Weiser supplies a complete description of security and device management features that are compatible with the system 700 of Iwami. EX1003, ¶126

B. Claim 7

1. [7a]

As discussed with respect to claims 1 and 2, Iwami in view of Kim and Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device, the permission includes connection information necessary for a connection, and the communication of such permission is through a short range communication. EX1003, ¶127

As discussed above, Liansky describes a process of connecting a mobile wireless device 120 and a screen device 110 for video streaming from the mobile wireless device 120 to the screen device 110 using transmission and receipt of a QR code (bar code) including connection information used to establish the connection. See limitation [2a] and [12a]. EX1012, FIG. 2, 5:3-37; EX1003, ¶128.

2. [7b]

As noted above, in the Iwami-Kim-Liansky system, the short range communication (i.e., the QR code) encodes address information such as a Mac address and/or an IP address. EX1012, FIG. 2, 5:3-37. See [2] and [7a] above. Kim also teaches sending address information, such as when control point 110 invokes the MulticastStart() action in communication S101, and media server 120 delivers a RTSP URL (RTSP server address) to control point 110 in response in communication S102. The RTSP URL is address information. EX1006, FIG. 1, [0036]; EX1007, FIG. 1, [0041]-[0042]; EX1003, ¶129.

Weiser also teaches transmitting address information. For example, Weiser teaches that a first client 602 and second client 606 may wish to communicate with one another but, in some cases, second client 606 does not know the IP address of first client 602. Opening a port and waiting for a connection exposes second client 606 to attack. EX1008, FIG. 6A, [0190]; EX1003, ¶130.

In the embodiment of FIG. 6B, Weiser introduces a system to solve this problem including a proxy/video conference bridge 608. Bridge 608 sends its own address information to first client 602 in response to an invitation sent by first client 602 intended for second client 606, such that first client 602 believes it is connected with second client 606 while in reality it is connected to bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶131.

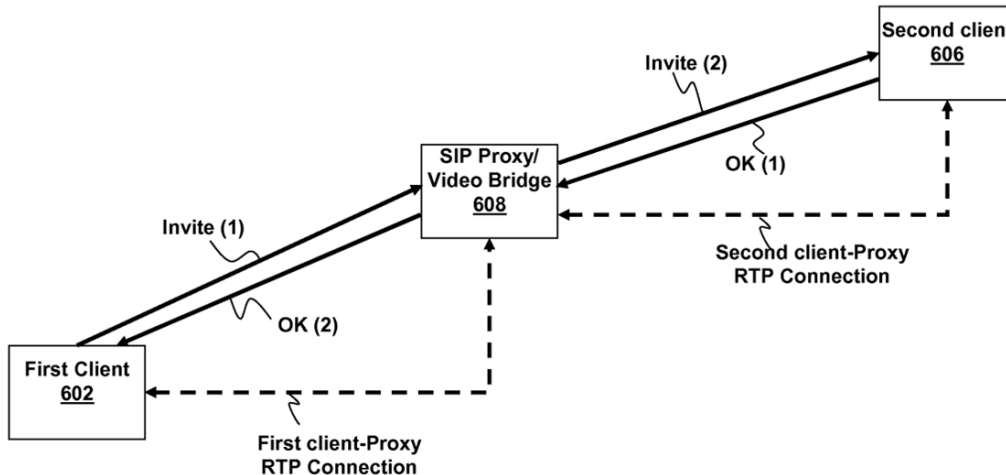


FIG. 6B

3. [7c]

In Weiser, first client 602 sends a message intended for second client 606 that includes an address of second client 606. Bridge 608 also sends its own address information to second client 606 in such a way that second client 606 believes it is connected with first client 602 while in reality it is connected to bridge 608. To summarize, a POSITA would have understood from Weiser that clients and/or bridges can send their own address information or address information of other devices to one another. EX1008, FIG. 6B, [0192]; EX1003, ¶132.

4. [7d]

Weiser teaches registering address information of the clients (e.g., clients 602 and/or 606) into a whitelist, or permission list. EX1008, FIG. 6B, [0194]; EX1003, ¶133.

5. [7e]

As discussed above with respect to claim 2, Iwami-Kim-Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device. Iwami-Kim-Liansky also teaches that the first communication terminal transmits connection information to the second communication terminal, the transmitting is through a short-range communication from the first communication terminal to the second communication terminal, and the second communication terminal connects to the communication device by using the connection information. EX1003, ¶134. See [1d] and [2].

As discussed above, in Liansky, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37; EX1003, ¶135.

Additionally, Weiser teaches that first client 602 and second client 606 connect with bridge 608 using information provided by bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶136.

6. [7f]

Weiser teaches that clients that are not allowed to connect to bridge 608 can be blacklisted. Weiser also teaches that being blacklisted may refer not only to being added to a blacklist, but being omitted from a whitelist. Accordingly, Weiser teaches adding a client address to a blacklist to explicitly deny connection permission, and this can include deleting the client address from the whitelist. EX1008, FIG. 6B, [0194], [0209]; EX1003, ¶137.

7. [7g]

Weiser teaches that blacklisting a client causes bridge 608 to deny communication requests from the client. Accordingly, deleting a client address from a whitelist will stop any communications from that client to bridge 608. EX1008, FIG. 6B, [0194]; EX1003, ¶138.

Based on Weiser's teachings, a POSITA would have been motivated to modify the system 700 of Iwami, alone or in view of Kim and Liansky, to configure any and/or all of the devices within system 700 to transmit connection information and/or address information, maintain a permissions list, and use the permissions list to enable or terminate connections between devices. A POSITA

would not necessarily send the exact sequence of messages to/from the exact sources/destinations specified by Weiser. Rather, a POSITA would have understood from Weiser that messages can include address information, and address information can be added to and/or removed from lists to control access permission. As discussed above, a POSITA would have been motivated to combine Iwami-Kim-Liansky with Weiser because they are in a same field of art, Iwami teaches that terminating permission is desirable, Kim describes a known technique for terminating such permission, and Weiser describes specific message content and white/blacklist techniques that a POSITA would reasonably expect to be successful when used in combination with one another. EX1003, ¶139

C. Claim 8

1. [8a]

As discussed above with respect to claims 1, 2, and 7, Iwami in view of Kim and Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device, the permission includes connection information necessary for a connection, and the communication of such permission is through a short range communication.

EX1003, ¶140

As discussed above, Liansky describes a process of connecting a mobile wireless device 120 and a screen device 110 for video streaming from the mobile

wireless device 120 to the screen device 110 using transmission and receipt of a QR code (bar code) including connection information used to establish the connection. See limitation [2a], [12a], and [7a]. EX1012, FIG. 2, 5:3-37; EX1003, ¶141.

2. [8b]

As noted above, in the Iwami-Kim-Liansky system, the short range communication (i.e., the QR code) encodes address information such as a Mac address and/or an IP address. EX1012, FIG. 2, 5:3-37. See [2] and [7a]. Kim also teaches sending address information, such as when control point 110 invokes the MulticastStart() action in communication S101, and media server 120 delivers a RTSP URL (RTSP server address) to control point 110 in response in communication S102. The RTSP URL is address information. EX1006, FIG. 1, [0036]; EX1007, FIG. 1, [0041]-[0042]; EX1003, ¶142. See also [7b].

As discussed at [7b], Weiser teaches transmitting address information by first client 602, second client 606, bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶143.

3. [8c]

Weiser teaches registering address information of the clients (e.g., clients 602 and/or 606) into a whitelist, or permission list. EX1008, FIG. 6B, [0194]; EX1003, ¶144. See also [7d] above.

4. [8d]

As discussed with respect to claims 2, and 7, Iwami-Kim-Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device. Iwami-Kim-Liansky also teaches that the first communication terminal transmits connection information to the second communication terminal, the transmitting is through a short range communication from the first communication terminal to the second communication terminal, and the second communication terminal connects to the communication device by using the connection information. EX1003, ¶145. See [1d], [2], and [7e].

As discussed above, in Liansky, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37; EX1003, ¶146.

Additionally, Weiser teaches that first client 602 and second client 606 connect with bridge 608 using information provided by bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶147.

5. [8e]

Weiser teaches that clients that are not allowed to connect to bridge 608 can be blacklisted. Weiser also teaches that being blacklisted may refer not only to being added to a blacklist, but being omitted from a whitelist. Accordingly, Weiser teaches adding a client address to a blacklist to explicitly deny connection permission, and this can include deleting the client address from the whitelist. EX1008, FIG. 6B, [0194], [0209]; EX1003, ¶148. See also [7f].

6. [8f]

Weiser teaches that the blacklist can be maintained by a device other than that which ultimately allows or denies the communication between the client and the bridge. For example, Weiser teaches a firewall of a device receiving a data packet from the client can determine to allow or deny the request. In some embodiments, the firewall makes the determination on its own. In other embodiments, the firewall makes the determination in combination with one or more security modules such as authentication engines, pinhole filters, or other modules. In the latter case, a POSITA would have understood that the firewall

must communicate with the one or more security modules to confirm whether to allow the connection. EX1008, [0200]; EX1003, ¶149.

7. [8g]

Weiser teaches that blacklisting a client causes bridge 608 to deny communication requests from the client. Accordingly, deleting a client address from a whitelist will stop any communications from that client to bridge 608. EX1008, FIG. 6B, [0194]; EX1003, ¶150. See also [7g] above.

Based on Weiser's teachings, a POSITA would have found it obvious to modify the system 700 of Iwami, alone or in view of Kim and Liansky, to configure any and/or all of the devices within system 700 to transmit connection information and/or address information, maintain a permissions list, and use the permissions list to enable or terminate connections between devices. A POSITA would not have found it necessary to send the exact sequence of messages to/from the exact sources/destinations specified by Weiser. Rather, a POSITA would have understood from Weiser that messages can include address information, and address information can be added to and/or removed from lists to control access permission. As discussed above, a POSITA would have been motivated to combine Iwami-Kim-Liansky with Weiser because they are in a same field of art, Iwami teaches that terminating permission is desirable, Kim describes a known technique for terminating such permission, and Weiser describes specific message content

and white/blacklist techniques that a POSITA would reasonably expect to be successful when used in combination with one another. EX1003, ¶151

D. Claim 10

1. [10a]

As discussed with respect to claims 1, 2, 7, and 8, Iwami in view of Kim and Liansky teaches devices communicating through a short range communication. As discussed above, Liansky describes a process of connecting a mobile wireless device 120 and a screen device 110 for video streaming from mobile wireless device 120 to screen device 110. In this process, screen device 110 displays a QR code (bar code), and mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication). EX1012, FIG. 2, 5:3-37; EX1003, ¶152.

2. [10b]

As discussed with respect to claims 1, 2, 7, and 8, Iwami in view of Kim and Liansky teaches sending connection information necessary for a connection. For example, when screen device 110 displays a QR code (bar code), the QR code includes parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information

obtained from the decoding to establish a wireless connection with screen device

110. EX1012, FIG. 2, 5:3-37; EX1003, ¶153.

3. [10c]

As noted above, Liansky and Weiser disclose transmitting address information. As discussed at [7b] and [8b], Liansky discloses short range communication between devices, wherein the short range communication is by a QR code including address information. EX1006, FIG. 1, [0036]; EX1007, FIG. 1, [0041]-[0042]; EX1003, ¶154-155.

As discussed at [7b] and [8b], Weiser also teaches transmitting address information by first client 602, second client 606, and bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶156.

4. [10d]

Weiser teaches registering address information of the clients (e.g., clients 602 and/or 606) into a whitelist, or permission list. EX1008, FIG. 6B, [0194]; EX1003, ¶157. See also [7d] and [8c].

5. [10e]

As discussed with respect to claims 1, 2, 7, and 8, Iwami-Kim-Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device. Iwami-Kim-Liansky also teaches that the first communication terminal transmits connection information to the second communication terminal, the transmitting is through a

short range communication from the first communication terminal to the second communication terminal, and the second communication terminal connects to the communication device by using the connection information. EX1003, ¶158 See [1d], [2], [7e], and [8d].

As discussed above, in Liansky, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37; EX1003, ¶159.

Additionally, Weiser teaches that client 602 and second client 606 connect with bridge 608 using information provided by bridge 608. EX1008, FIG. 6B, [0192]; EX1003, ¶160.

6. [10f]

Weiser teaches that clients that are not allowed to connect to bridge 608 can be blacklisted. Weiser also teaches that being blacklisted may refer not only to being added to a blacklist, but being omitted from a whitelist. Accordingly, Weiser teaches adding a client address to a blacklist to explicitly deny connection

permission, and this can include deleting the client address from the whitelist.

EX1008, FIG. 6B, [0194], [0209]; EX1003, ¶161. See also [7f] and [8e].

7. [10g]

Weiser teaches that blacklisting a client causes bridge 608 to deny communication requests from the client. Accordingly, deleting a client address from a whitelist will stop any communications from that client to bridge 608.

EX1008, FIG. 6B, [0194]; EX1003, ¶162. See also [7g] and [8g].

Based Weiser's teachings, a POSITA would have found it obvious to modify the system 700 of Iwami to configure any and/or all of the devices within system 700 to transmit connection information and/or address information, maintain a permissions list, and use the permissions list to enable or terminate connections between devices. A POSITA would not necessarily send the exact sequence of messages to/from the exact sources/destinations specified by Weiser. Rather, a POSITA would have understood from Weiser that messages can include address information, and address information can be added to and/or removed from lists to control access permission. As discussed above, a POSITA would have been motivated to combine Iwami-Kim-Liansky with Weiser because they are in a same field of art, Iwami teaches that terminating permission is desirable, Kim describes a known technique for terminating such permission, and Weiser describes specific

message content and white/blacklist techniques that a POSITA would reasonably expect to be successful when used in combination with one another. EX1003, ¶163

IX. GROUND 4: CLAIMS 9 AND 11 ARE OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF LIANSKY AND KATO

A. Proposed Combination and Motivation to Combine

Iwami, alone or as modified by Kim, teaches that devices can request to connect to other devices in a network, and such connections are allowed or terminated based on permissions. EX1004, [0318]-[0322] , [0406]-[0407], [0448]-[0455]; EX1005, [0266]-[0270], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]; EX1003, ¶164.

A POSITA would have found it obvious, and would have been motivated to, modify the Iwami-Kim-Liansky system by implementing a one-time password element of the Kato security techniques to provide connection security within the system 700 of Iwami as discussed in further detail below. The provisioning and use of a one-time password can help control device 740 determine whether to enable and/or disable connections by information processing devices 703, 704, 710, and/or 720. Doing so would have simply involved combining known prior art elements (i.e., system 700 elements of Iwami, alone or in view of Kim and Liansky) according to known methods (i.e., the security features of Kato) to yield predictable results (i.e., a system 700 whose elements can communicate with one

another, or not, based on permission or lack thereof with one-time password features to enhance security). EX1003, ¶164

Iwami, Kim, Liansky and Kato are analogous art and are directed toward the same or similar problems. For example, as noted above, Iwami and Kim both relate to media transmission and display in a network environment and both discuss using permission to control connections between devices in the network environment, and Liansky relates to additional permission and/or security controls for the connections in the same or similar network environment. EX1004, (57), [0002], [0009], [0406]-[0407], [0448]-[0455]; EX1005, [Abstract], [0001], [0008], [0330]-[0331], [0372]-[0377]; EX1006 (57), [0001], [0018], [0037]-[0045]; EX1007, [0007], [0020]-[0028], [0043]-[0052]; EX1012, (57), 1:32-49, 2:5-24. Similarly, Kato is directed to network communication, including communication management features that determine whether to permit a requested connection between network devices. EX1009, (57), [0008], [0009]; EX1010, [0005]-[0008]; EX1011, [0005]-[0008]. Kato describes security features that enable determination whether to permit a connection, including one-time password generation and use. EX1009, [0082]-[0083], [0086]-[0090]; EX1010, [0056]-[0057], [0059]-[0062]; EX1011, [0059]-[0060], [0063]-[0066]; EX1003, ¶165.

A POSITA would have been capable of modifying Iwami's system 700 (considered alone or as modified by Kim, Liansky, and/or a POSITA's

knowledge), and individual elements thereof and/or actions performed by those elements, by the Kato's teachings, and would have had a reasonable expectation of success in so doing because such modifications require only ordinary skill.

Additionally, a POSITA would have understood that Kato supplies a complete description of security features that are compatible with the system 700 of Iwami.

EX1003, ¶166

B. Claim 9

1. [9a]

Iwami teaches source device 710 (the second communication terminal) sending a GO_Negotiation_Request (or “group owner” negotiation request) to sink device 730 (the communication device) and receiving a GO_Negotiation_Response from sink device 730. After the GO_Negotiation_Response message is sent, the two devices in communication with one another share credentials. EX1004, FIG. 24, [0319]-[0322]; EX1005, FIG. 24, [0267]-[0270]; EX1003, ¶167.

In Iwami, the above-cited communication is between the second communication terminal and the communication device. However, Iwami also teaches that control device 740 and source devices 703, 704, 710, and 720 all use the same network (i.e., the wireless LAN) to communicate with sink device 730. Iwami also teaches that control device 740 has a protocol for establishing a

connection with access point 701 and with sink device 730 via access point 701.

EX1004, [0246], [0250]; EX1005, [0197], [0201]. At minimum, Iwami teaches a protocol for establishing a connection between the first communication terminal and the communication device, which a POSITA would have understood to include exchange of messages. Given that control device 740 can communicate with sink device 730 on the same network source device 710 communicates with sink device 730, control device 740 could send similar GO_Negotiation_Response messages and exchange credentials to establish connection. EX1003, ¶168

After the GO_Negotiation_Response message is sent, the two devices in communication with one another share credentials. Iwami does not specifically teach that the credentials can include a one-time password giving permission. Kato discloses a communication system 500 including communication apparatus 10da and external input device 40da. The communication apparatus 10da includes a password generation unit 610 that generates a one-time password that is included in login information. The communication apparatus 10da also includes a display unit 603 that displays the login information. EX1009, FIG. 6, [0082]-[0083], [0086], [0088]; EX1010, FIG. 6, [0056]-[0057], [0059], [0061]; EX1011, [0059]-[0060], [0063], [0065]. It would have been obvious to modify Iwami's credential exchange to include a one-time password as at least one of the credentials. A POSITA would have been motivated to require a one-time password as taught by

Kato to ensure that the communication being attempted is permitted during the present session, which both Iwami and Kato describe as desirable. EX1004, [0273], [0407]; EX1005, [0224], [0331]; EX1009, [0089]; EX1010, [0061]; EX1011, [0065]; EX1003, ¶169.

2. [9b]

As discussed with respect to claims 1, 2, 7, and 8, Iwami in view of Kim and Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device, the permission includes connection information necessary for a connection, and the communication of such permission is through a short range communication.

EX1003, ¶170

As discussed above, Liansky describes a process of connecting mobile wireless device 120 and screen device 110 for video streaming from the mobile wireless device 120 to screen device 110. In this process, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a

wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37. As discussed above and disclosed by Kato, the information sent by short range communication can include the one-time password used as connection information by Kato's system, and it would have been obvious to give the same password for the same session to both the first communication terminal and the second communication terminal to allow them to both connect during the same session. EX1009, FIG. 6, [0082]-[0083], [0086], [0088]; EX1010, FIG. 6, [0056]-[0057], [0059], [0061]; EX1011, [0059]-[0060], [0063], [0065]; EX1003, ¶171. See claim 2 and limitation [9a].

3. [9c]

As discussed with respect to claims 1, 2, 7, and 8, Iwami-Kim-Liansky teaches a first communication terminal giving permission to a second communication terminal to connect with a communication device. Iwami-Kim-Liansky also teaches that the first communication terminal transmits connection information to the second communication terminal, the transmitting is through a short range communication from the first communication terminal to the second communication terminal, and the second communication terminal connects to the communication device by using the connection information. EX1003, ¶172. See [1d], [2], [7e], and [8d].

As discussed above, in Liansky, screen device 110 displays a QR code (bar code) including parameters such as Mac address, SSID, WiFi encryption key, PIN code, IP address, and/or stream encryption key (connection information necessary for a connection represented by the bar code). The mobile wireless device 120 captures an image of the QR code using its camera (i.e., the two devices perform a short range communication), decodes the image, and uses the connection information obtained from the decoding to establish a wireless connection with screen device 110. EX1012, FIG. 2, 5:3-37. Moreover, when the connection information includes a one-time password as taught by Kato, the device receiving the one-time password uses the one-time password to connect. For example, in Kato, server unit 608 of communication apparatus 10da supplies a web page to external input device 40da. The web page accepts input of the one-time password and, based on correct entry of the one-time password, a login authentication unit 609 of communication apparatus 10da permits login by communication apparatus 10da. EX1009, FIG. 6, [0082]-[0083], [0089]-[0090]; EX1010, FIG. 6, [0056]-[0057], [0061]-[0062]; EX1011, [0059]-[0060], [0065]-[0066]; EX1003, ¶173.

C. Claim 11

1. [11a]

Iwami teaches source device 710 (the second communication terminal) sending a GO_Negotiation_Request to sink device 730 (the communication

device) and receiving a GO_Negotiation_Response from sink device 730. After the GO_Negotiation_Response message is sent, the two devices in communication with one another share credentials. EX1004, FIG. 24, [0319]-[0322]; EX1005, FIG. 24, [0267]-[0270]; EX1003, ¶174. See [9a].

After the GO_Negotiation_Response message is sent, the two devices in communication with one another share credentials. Iwami does not specifically teach that the credentials can include a one-time password giving permission. Kato discloses a communication system 500 including communication apparatus 10da and external input device 40da. The communication apparatus 10da includes password generation unit 610 that generates a one-time password that is included in login information. The communication apparatus 10da also includes display unit 603 that displays the login information. EX1009, FIG. 6, [0082]-[0083], [0086], [0088]; EX1010, FIG. 6, [0056]-[0057], [0059], [0061]; EX1011, [0059]-[0060], [0063], [0065]. It would have been obvious to modify Iwami's credential exchange to include a one-time password as at least one of the credentials. A POSITA would have been motivated to require a one-time password as taught by Kato to ensure that the communication being attempted is permitted during the present session, which both Iwami and Kato describe as desirable. EX1004, [0273], [0407]; EX1005, [0224], [0331]; EX1009, [0089]; EX1010, [0061]; EX1011, [0065]; EX1003, ¶175.

2. [11b]

As discussed above, after the GO_Negotiation_Response message is sent, the two devices in communication with one another share credentials, indicating that the communication device transmits information to the second communication terminal. Iwami does not specifically teach that the credentials can include a one-time password giving permission. However, as discussed above and disclosed by Kato, the information sent by the communication device can include the one-time password used as connection information by Kato's system. EX1009, FIG. 6, [0082]-[0083], [0086], [0088]; EX1010, FIG. 6, [0056]-[0057], [0059], [0061]; EX1011, [0059]-[0060], [0063], [0065]; EX1003, ¶176. See [2], [9a], [9b], and [11a].

3. [11c]

See [11c] above; see also EX1003, ¶177-178.

X. GROUND 5: CLAIM 6 IS OBVIOUS OVER IWAMI AND KIM IN FURTHER VIEW OF DOWLING

A. Motivation to Combine

A POSITA would have found it obvious, and would have been motivated to, modify the Iwami-Kim system by incorporating elements of the Dowling network management techniques, such as local network connection management and maintenance features, to maintain connection status for devices within system 700 of Iwami. EX1003, ¶179.

In particular, Dowling discloses using a periodic heartbeat packet sent from member devices to a commander device to enable the commander device to detect when a member device has become inactive so that the connection of the member device can be terminated to keep the number of connections low. EX1021, 19:31-48. In view of this teaching, a POSITA would have found it obvious to configure Iwami's source information processing devices 710, 720 to periodically transmit a heartbeat packet when in standby mode to sink device 730 to enable it to detect when connections to devices 710, 720 should be terminated. In standby mode, the source devices 710, 720 are not transmitting video and thus would be understood to have minimal communications with sink device 730. EX1004, [0270], [0289]-[0290]; EX1005, [0221], [0240]-[0241]. Also, in a classroom setting as contemplated by Iwami, such as a university lecture hall environment, a POSITA would have understood that students will be transitory, and thus it would be desirable to terminate connections for student devices 710, 720 when those students and their devices leave a classroom and the range of the access point 701. Indeed, Iwami describes connecting student devices 710, 720 upon check-in using near-field communication, where a student touches a device to an NFC reader. This indicates these devices are not always present in the classroom but rather are coming and going. EX1004, [0256], [0351], [0435]-[0442]; EX1005, [0207], [0359]-[0366]. A POSITA would have understood that detecting the absence of a

heartbeat signal from a student device 710, 720 would be a suitable technique for detecting such departures and terminating those connections. Doing so would have simply involved combining known prior art elements (i.e., the system 700 elements of Iwami, alone or in view of Kim) according to known methods (i.e., the local network management features of Dowling) to yield predictable results. A POSITA would have had a reasonable expectation of success because heartbeat signals were well-known in the art and modifying Iwami in this manner involved only routine skill. EX1003, ¶180-181.

B. Claim 6

1. [6a]

See limitations [1c], [1e] and [1f] above. Causing the image from a selected information processing device to be moved from the peripheral channel region 734 to the middle channel region 733 as described in those sections satisfies this limitation. EX1003, ¶182-184.

2. [6b]

See V.B.2. A POSITA would have known that if access point 701 stops working to provide the wireless LAN (e.g., due to a malfunction or power loss), it would create a case where the communication device (sink device 730) is unable to receive information from the first communication terminal (control device 740). EX1003, ¶185-188. In that case, heartbeat packets from a source device 710, 720 in the Iwami-Kim-Dowling system will not be received through the access point

701 by sink device 730, which would respond by terminating the connection to source device 710, 720 as discussed above in Section X.A.

XI. MANDATORY NOTICES UNDER 37 C.F.R. §§ 42.8(B)(1)-(4)

A. Real Parties-In-Interest

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. are the real parties-in-interest.

B. Related Matters

The '088 patent is subject of the following action: *Maxell Ltd. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, No. 5:25-cv-00052-RWS (E.D. Tex.).

C. Lead and Backup Counsel

Lead Counsel	Backup Counsel
James M. Heintz Reg. No. 41,828 DLA Piper LLP One Fountain Square 11911 Freedom Drive, Suite 300 Reston, VA 20190-5602 Phone: + 1 703 773 4000 Fax: + 1 703 773 5000 Jim.heintz@us.dlapiper.com	Nicholas Panno Reg. No. 68,513 DLA Piper LLP 701 Fifth Avenue Suite 6900 Seattle, WA 98104-7029 Phone: + 1 206 839 4800 Fax: + 1 206 839 4801 Nicholas.panno@us.dlapiper.com

D. Service Information

Service information for lead and backup counsel is provided in the designation of lead and backup counsel above. Petitioner consents to electronic service to lead and back-up counsel and to: DLA-Maxell-ITC IPRs@us.dlapiper.com

XII. CONCLUSION

All Challenged Claims of the '088 patent should be found unpatentable for the reasons discussed in this Petition.

Date: July 25, 2025

Respectfully submitted,

/s/ James Heintz

Reg. No. 41828

DLA Piper LLP

One Fountain Square

11911 Freedom Drive, Suite 300

Reston, VA 20190-5602

Phone: + 1 703 773 4000

Fax: + 1 703 773 5000

Jim.heintz@us.dlapiper.com

Attorney for Petitioners

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner certifies that this petition includes 13,931 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under § 42.8, certificates of service, word count, claim listing, and exhibits.

Date: July 25, 2025

s/ James M. Heintz
James M. Heintz
Reg. No. 41,828
DLA Piper LLP
One Fountain Square
11911 Freedom Drive, Suite 300
Reston, VA 20190-5602
Phone: + 1 703 773 4000
Fax: + 1 703 773 5000
jim.heintz@us.dlapiper.com

Attorney for Petitioners

CERTIFICATE OF SERVICE

The undersigned certifies pursuant to 37 C.F.R. §§ 42.6(e) and 42.105 that on July 25, 2025, a true and correct copy of the Petition for *Inter Partes* Review of U.S. Patent No. 11,026,088 was served was served by emailing a copy of the same (by agreement) to the following attorneys for the Patent Owner:

Robert G. Pluta – rpluta@mayerbrown.com

Saqib Siddiqui – ssiddiqui@mayerbrown.com

A courtesy copy was sent to the counsel below via electronic mail:

maxell-samsung-service@mayerbrown.com

Respectfully submitted,

/s/ James M. Heintz

James M. Heintz

Reg. No. 41,828

DLA Piper LLP

One Fountain Square

11911 Freedom Drive, Suite 300

Reston, VA 20190-5602

Phone: + 1 703 773 4000

Fax: + 1 703 773 5000

jim.heintz@us.dlapiper.com

Attorney for Petitioners