

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZOOM COMMUNICATIONS, INC.
Petitioner

v.

RICOH COMPANY, LTD.
Patent Owner

IPR2026-00453

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 10,931,917**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. TECHNOLOGY BACKGROUND.....	2
A. Video Conferencing Between Authenticated Terminals via Relay Servers Was Well-Known.....	2
B. Sharing Content and Display Data During Video Conferences Was Well-Known	5
C. Connecting External Input Devices to Conference Terminals Without Requiring Separate Authentication Was Well-Known.....	8
D. Transmitting Multiple Types of Data Over an Established Communication Session Was Well-Known.....	8
E. Transmitting Programs to Connected Peripheral Devices Upon Connection, with Conditional Installation, Was Well-Known	10
III. '917 PATENT.....	12
A. Overview	12
B. Prosecution History	14
IV. POSITA	16
V. CLAIM CONSTRUCTION	17
VI. OVERVIEW OF CHALLENGE.....	17
VII. THE ASSERTED GROUNDS OF INVALIDITY	18
A. Ground 1: Toya in view of Tucker Renders Obvious Claims 1-3, 7-10, 14-15	18
1. Motivation to Combine	19
2. Preambles	24
a) [1.pre].....	24
b) [8.pre].....	26
c) [15.pre].....	27

TABLE OF CONTENTS

(continued)

	Page
3. [1.a]/[8.a]/[15.a]	29
4. [1.b]/[8.b]/[15.b]	30
5. [1.c]/[8.c]/[15.c]	33
6. [1.d]/[8.d]/[15.d]	34
7. [1.e]/[8.e]/[15.e]	36
8. [1.f]/[8.f]/[15.f]	41
9. Claim 2/9.....	42
10. [3.a]/[10.a].....	46
11. [3.b]/[10.b]	48
12. [7.a]/[14.a].....	51
13. [7.b]/[14.b]	54
14. [7.c]/[14.c].....	55
 B. Ground 2: Toya in view of Tucker and Further in View of Chang Renders Obvious Claims 4-6, 11-13	 56
1. Motivation to Combine	59
2. [4.a]/[11.a].....	62
3. [4.b]/[11.b]	67
4. Claim 5/12.....	69
5. Claim 6/13.....	70
 C. Ground 3: Toya in view of RFC 3261 Renders Obvious Claims 1-3, 8-10, 15	 72
1. RFC 3261	72
2. Motivation to Combine	75

TABLE OF CONTENTS
(continued)

	Page
3. [1.b]/[8.b]/[15.b]	79
D. Ground 4: Toya in view of RFC 3261 and Further in View of Chang Renders Obvious Claims 4-6	81
1. Motivation to Combine	83
2. [4.a]/[11.a]	88
3. [4.b]/[11.b]	88
4. Claim 5/12	89
5. Claim 6/13	89
VIII. CONCLUSION	89
IX. MANDATORY NOTICES PURSUANT TO 37 C.F.R. §42.8	89
A. Real Parties-In-Interest under 37 C.F.R. §42.8(b)(1).	89
B. Related Matters Under 37 C.F.R. §42.8(b)(2).	89
C. Lead and Back-up Counsel under 37 C.F.R. §42.8(b)(3).	89
D. Service Information under 37 C.F.R. §42.8(b)(4)	90
X. GROUNDS FOR STANDING	90
XI. PAYMENT OF FEES	91
XII. STATEMENT OF PRECISE RELIEF REQUESTED	91

TABLE OF AUTHORITIES

Page(s)

Cases

<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	<i>passim</i>
---	---------------

Statutes

35 U.S.C. §102.....	17
35 U.S.C. § 102(b)	18, 73
35 U.S.C. §103.....	14, 17, 91

Other Authorities

37 C.F.R. §1.312	15
37 C.F.R. §42.8	89
37 C.F.R. §42.8(b)(1).....	89
37 C.F.R. §42.8(b)(2).....	89
37 C.F.R. §42.8(b)(3).....	89
37 C.F.R. §42.8(b)(4).....	90
37 C.F.R. §42.15(a).....	91
37 C.F.R. §42.103	91
37 C.F.R. §42.104(a).....	90

PETITIONER’S EXHIBIT LIST

No.	Reference	Referred To As
1001	U.S. Patent No. 10,931,917	'917 Patent
1002	Prosecution History of U.S. Patent No. 10,931,917	'917 Patent File History
1003	Declaration of Dr. Kevin Almeroth	Almeroth Decl.
1004	U.S. Patent No. 8,305,422	Toya
1005	U.S. Patent Application Publication No. 2010/0066805	Tucker
1006	RFC 3261 - SIP: Session Initiation Protocol	RFC 3261
1007	U.S. Patent No. 8,316,138	Chang
1008	U.S. Patent No. 7,373,379	Comstock
1009	U.S. Patent No. 8,264,520	Oya
1010	U.S. Patent No. 7,035,899	Marchon
1011	U.S. Patent No. 6,760,749	Dunlap
1012	U.S. Patent Application Publication No. 2012/0133727	Bolduc
1013	U.S. Patent No. 7,668,986	Lowe
1014	U.S. Patent No. 8,190,785	Hill
1015	U.S. Patent No. 8,260,978	Thompson
1016	SMART Technologies ULC’s International Publication No. WO 2010/105335	Banerjee
1017	NISP Nation_NISP Standard-RFC 3261.pdf	NISP Nation
1018	Internet Engineering Task Force (IETF) IANA Registry – Updating 3261	IANA Registry – Updating 3261
1019	G. Banks, M. Cova, V. Felmetsger, K. Almeroth, R. Kemmerer and G. Vigna, " SNOOZE: toward a Stateful NetwOrk prOtocol fuzZEr ," <i>Information Security Conference (ISC)</i> , Samos Island, GREECE, September 2006.	Banks
1020	U.S. Pat. Publ. No. 2004/0062204A1	Bearden

LISTING OF CHALLENGED CLAIMS

Claim	Limitation
[1.pre]	A first transmission terminal comprising: processing circuitry configured to
[1.a]	obtain first video data captured by a camera,
[1.b]	log into a management system by transmitting a login request to the management system,
[1.c]	establish a communication session for transmitting the first video data to a second transmission terminal that has logged into the management system,
[1.d]	transmit the first video data using the established communication session
[1.e]	when an external input apparatus that has not logged into the management system is connected with the first transmission terminal during the first video data being displayed on a display screen of the second transmission terminal, receive, from the external input apparatus, second video data obtained in the external input apparatus, and
[1.f]	in response to receiving the second video data, transmit the first video data and the second video data for sharing with the second transmission terminal using the established communication session.
[2]	The first transmission terminal according to claim 1, wherein the processing circuitry is configured to transmit the first video data and the second video data via a relay apparatus.
[3.a]	The first transmission terminal according to claim 2, wherein the relay apparatus is selected from a plurality of relay apparatuses, and

[3.b]	the processing circuitry receives, from the management system, terminal identification information for identifying another transmission terminal that has requested a start of communication from among a plurality of transmission terminals.
[4.a]	The first transmission terminal according to claim 1, wherein the processing circuitry receives, from the external input apparatus, a request for permission to execute a program that is for obtaining data in the external input apparatus, and
[4.b]	in response to permission of the request, the program is executed in the external input apparatus, and thus, the processing circuitry receives, from the external input apparatus, the second video data obtained in the external input apparatus.
[5]	The first transmission terminal according to claim 4, wherein the processing circuitry is configured to transmit the program to the external input apparatus.
[6]	The first transmission terminal according to claim 5, wherein if the program is not installed in the external input apparatus when the first transmission terminal is connected with the external input apparatus, the processing circuitry transmits the program to the external input apparatus.
[7.a]	The first transmission terminal according to claim 1, wherein the processing circuitry is configured to receive, from the management system, information of destination candidates associated with the first transmission terminal,
[7.b]	receive a selection from among the received information of the destination candidates, and

[7.c]	establish the communication session with the second transmission terminal corresponding to information of the thus selected destination candidate.
[8.pre]	A method, implemented by a first transmission terminal, comprising:
[8.a]	obtaining first video data captured by a camera,
[8.b]	logging into a management system by transmitting a login request to the management system,
[8.c]	establishing a communication session for transmitting the first video data to a second transmission terminal that has logged into the management system,
[8.d]	transmitting the first video data using the established communication session,
[8.e]	when an external input apparatus that has not logged into the management system is connected with the first transmission terminal during the first video data being displayed on a display screen of the second transmission terminal, receiving, from the external input apparatus, second video data obtained in the external input apparatus, and
[8.f]	in response to receiving the second video data, transmitting the first video data and the second video data for sharing with the second transmission terminal using the established communication session.
[9]	The method according to claim 8, further comprising transmitting the first video data and the second video data via a relay apparatus.
[10.a]	The method according to claim 9, wherein the relay apparatus is selected from a plurality of relay apparatuses, and

[10.b]	the method includes receiving, from the management system, terminal identification information for identifying another transmission terminal that has requested a start of communication from among a plurality of transmission terminals
[11.a]	The method according to claim 8, further comprising: receiving, from the external input apparatus, a request for permission to execute a program that is for obtaining data in the external input apparatus, and
[11.b]	in response to permission of the request, the program is executed in the external input apparatus, and thus, the method includes receiving, from the external input apparatus, the second video data obtained in the external input apparatus.
[12]	The method to claim 11, further comprising transmitting the program to the external input apparatus.
[13]	The transmission terminal according to claim 12, further comprising: if the program is not installed in the external input apparatus when the transmission terminal is connected with the external input apparatus, transmitting the program to the external input apparatus.
[14.a]	The method according to claim 8, further comprising: receiving, from the management system, information of destination candidates associated with the first transmission terminal;
[14.b]	receiving a selection from among the received information of the destination candidates; and

[14.c]	establishing the communication session with the second transmission terminal corresponding to information of the thus selected destination candidate.
[15.pre]	A non-transitory computer readable medium that stores a program that when executed by a first transmission terminal causes the first transmission terminal to perform a method comprising:
[15.a]	obtaining first video data captured by a camera,
[15.b]	logging into a management system by transmitting a login request to the management system,
[15.c]	establishing a communication session for transmitting the first video data to a second transmission terminal that has logged into the management system,
[15.d]	transmitting the first video data using the established communication session,
[15.e]	when an external input apparatus that has not logged into the management system is connected with the first transmission terminal during the first video data being displayed on a display screen of the second transmission terminal, receiving, from the external input apparatus, second video data obtained in the external input apparatus, and
[15.f]	in response to receiving the second video data, transmitting the first video data and the second video data for sharing with the second transmission terminal using the established communication session.

I. INTRODUCTION

Petitioner requests *inter partes* review and cancellation of claims 1-15 of U.S. Patent No. 10,931,917 (“the ’917 Patent”) (EX1001). The ’917 Patent is directed to letting a video-conferencing terminal share data from a connected device that has not separately logged into the management system. The challenged claims describe a simple, familiar interaction: two authenticated video-conferencing terminals start a call and exchange camera video, a user plugs a laptop or other device into one terminal, and that terminal sends the device's data to the other participant alongside its own camera video. This merely combines three known components: (1) a video-conferencing terminal that logs into a server; (2) an established video-call session between authenticated terminals that exchange camera video; and (3) forwarding data from a plugged-in device that has not separately logged in. The claimed step is simple: plug in a device and forward its data over the existing call.

Every element of the claimed interaction was known before May 6, 2010. Toya (EX1004) discloses the video-conferencing terminal that receives external content and forwards it over an established session; Tucker (EX1005) discloses server-based user authentication before video conferencing; RFC 3261 (EX1006) discloses SIP registration and authentication through registrars; and Chang (EX1007) discloses automatically delivering screen-capture software from a hub to an external laptop upon USB connection. The ’917 Patent adds no technological

leap; it merely routes ordinary data from a connected device through a terminal already participating in an authenticated video call.

Petitioner therefore respectfully requests institution of *inter partes* review and cancellation of all claims of the '917 Patent.

II. TECHNOLOGY BACKGROUND

The '917 Patent relates to a transmission terminal that logs into a management system, establishes a video conference session with a second terminal, and—when an external input apparatus that has not logged into the management system is connected—forwards the external apparatus's display data alongside the terminal's own camera video to the second terminal over the already-established session. *See* EX1001, claims 1, 8, 15. Every aspect of this technology was well-known years before the earliest possible priority date of May 6, 2010. EX1003, ¶27.

A. Video Conferencing Between Authenticated Terminals via Relay Servers Was Well-Known

Relay-based conferencing architectures—in which an intermediary server routes media streams between endpoints—were the predominant model prior to the '917 Patent. EX1003, ¶[28]. Polycom's U.S. Patent No. 7,373,379 (Comstock) taught the use of MCUs for “switching and multiplexing video, audio, and data streams in a multimedia conference.” EX1008, 4:60-5:9, FIGS1-2. Tucker et al. (U.S. Patent Application Publication No. 2010/0066805) likewise taught a server-

mediated video conference system handling authentication, invitation management, and data relay. EX1005; EX1003, ¶[28].

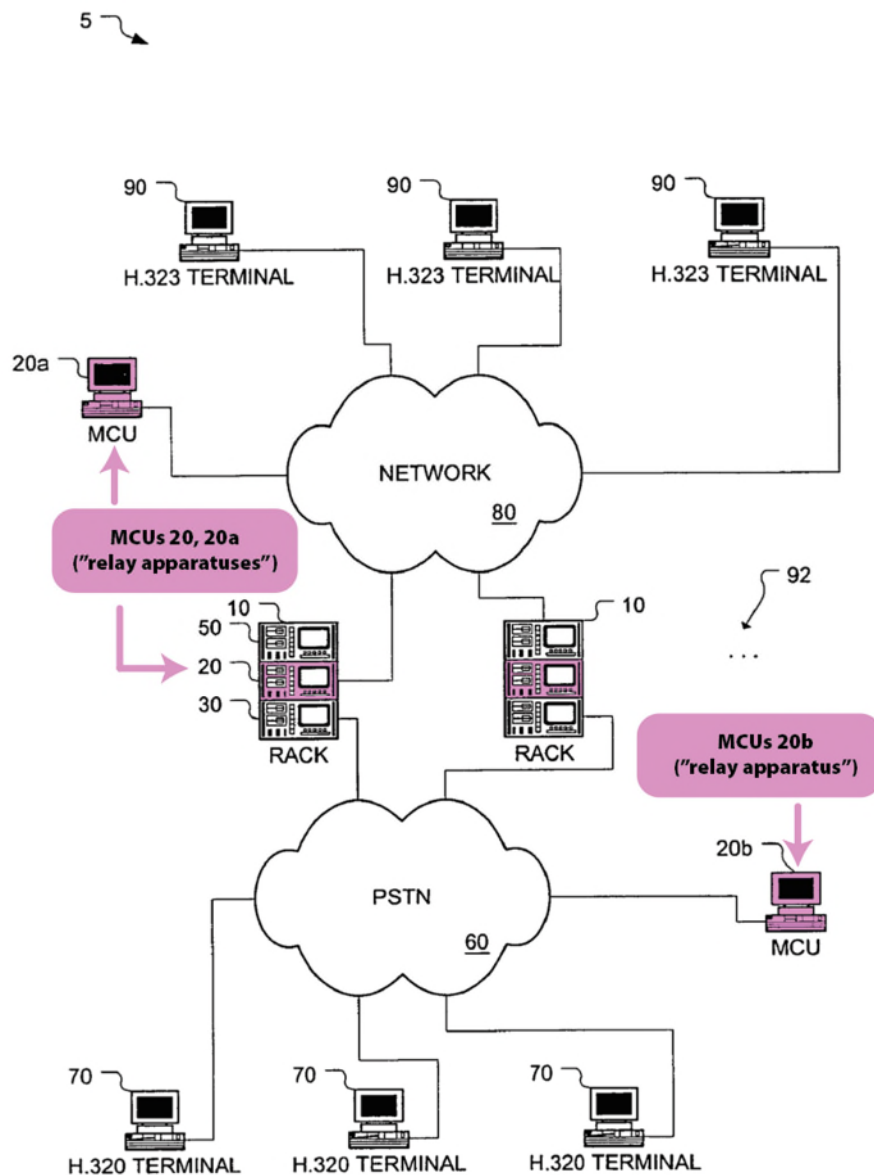
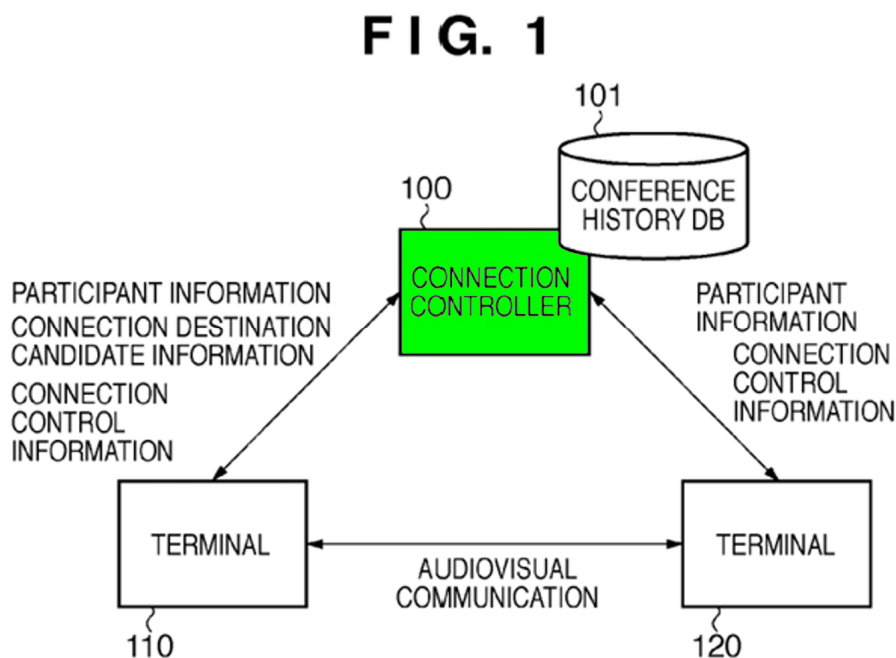


FIG. 1

EX1008, FIG1.

Requiring terminals to authenticate with a management system before joining a conference was equally well-known. EX1003, ¶[29]. Canon's U.S. Patent No. 8,264,520 (Oya) describes a connection controller that manages terminal authentication, connection candidates, and session establishment. EX1009, Abstract, FIGS. 1-6 1:8-28, 1:66-2:2, 3:41-4:26. U.S. Patent No. 7,035,899 (Marchon) similarly requires user authentication before establishing a meeting session, with the server validating credentials and generating access tokens. EX1010, Abstract, 8:65-9:39, FIG.9. A POSITA would have understood that authenticating terminals through a management system before permitting conference participation was well-known. EX1003, ¶[29].



EX1009, FIG1.

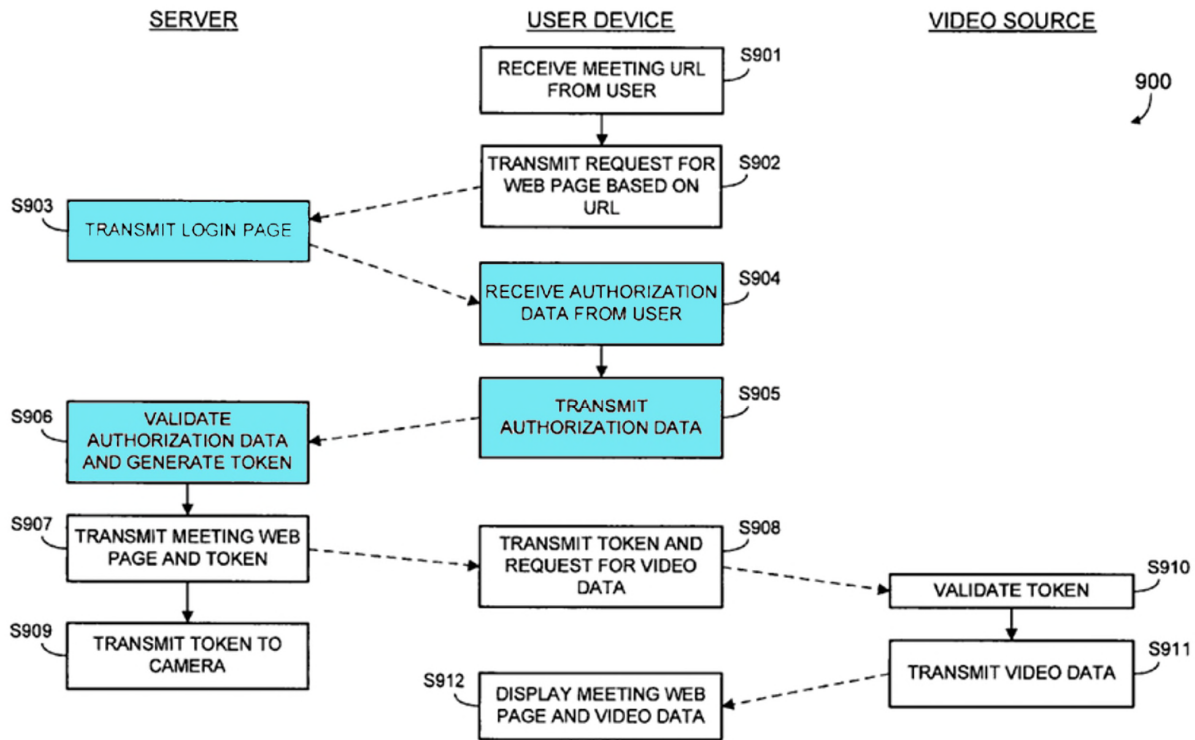


FIG. 9

EX1010, FIG9.

B. Sharing Content and Display Data During Video Conferences Was Well-Known

The ‘917 Patent acknowledges that sharing “presentation content” during video conferences was known, citing U.S. Pat. No. 6,760,749 (Dunlap) (EX1011), which “discusses a technology whereby the display data of a material . . . is transmitted together with the audio and video data to a distributing apparatus [relay apparatus] during a telephone conference via a network.” EX1001, 1:61-2:3; EX1003, ¶30.

Toya teaches a conference terminal that obtains content data from outside sources and automatically transmits it to the conferencing counterpart once a call session is established—without requiring the user to specify the device. EX1004, Abstract, 18:24-41, 20:54-21:37. Comstock further teaches explicitly assigning “content” and “people” roles to media streams, with separate source switches handling inputs from computers and document cameras alongside live camera video. EX1008, 5:20-8:31, FIG2. Content sharing during conferences was thus ubiquitous in the prior art. EX1003, ¶31.

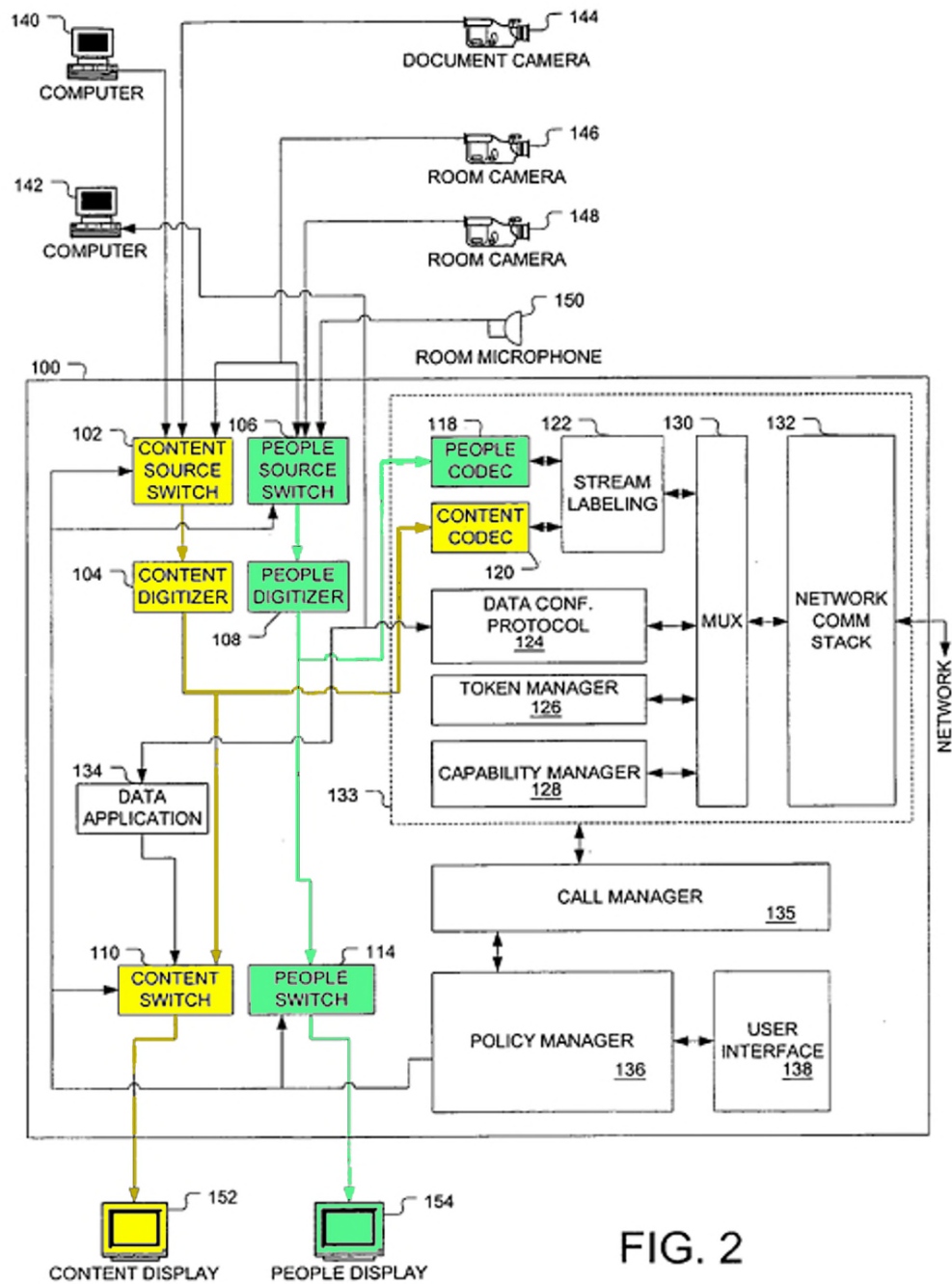


FIG. 2

EX1008, FIG2.

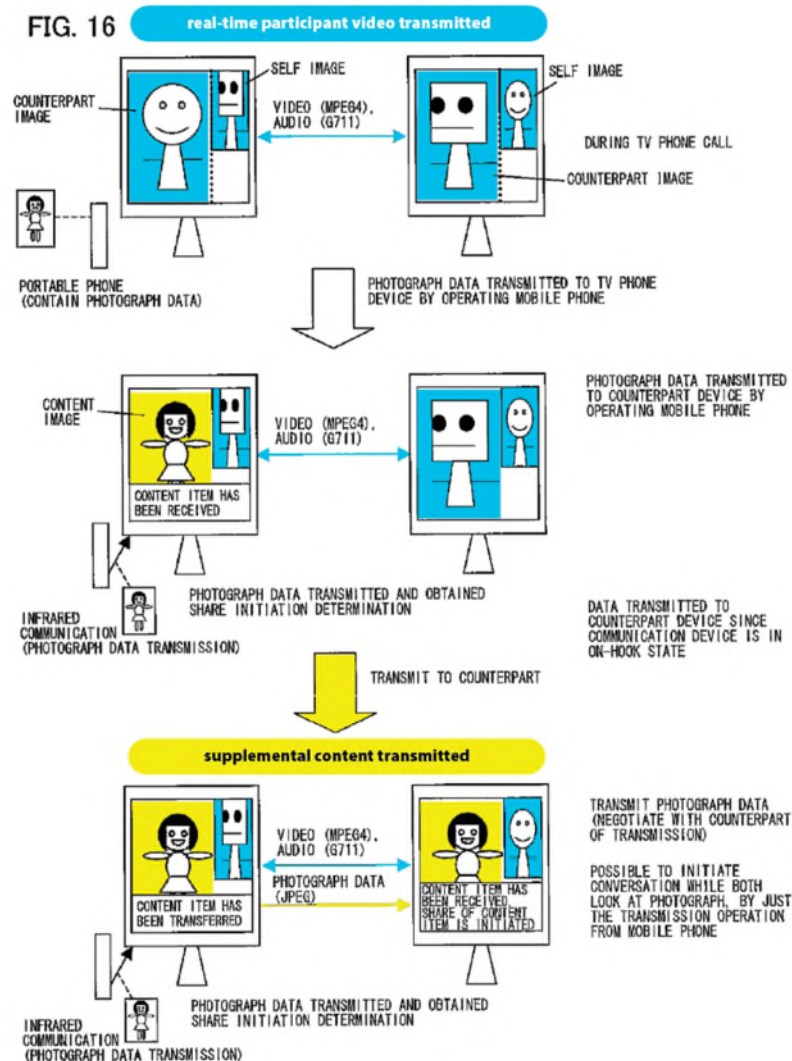
C. Connecting External Input Devices to Conference Terminals Without Requiring Separate Authentication Was Well-Known

This gateway pattern of forwarding data through the same relay apparatus carrying the video conference traffic was well-known at the time of the '917 Patent. EX1003, ¶32. Toya receives content from external sources via Bluetooth, infrared, ethernet and SD card interfaces and forwards it to the conferencing counterpart—without requiring the external source to authenticate with or connect to any management system. EX1004, 18:42-21:20. In Comstock, computers and document cameras connect directly to the terminal's content source switch, and their output is digitized, encoded, and transmitted to remote endpoints without those devices independently registering with the conferencing network. EX1008, 5:20-6:50, FIG2. A POSITA would have recognized that using a conference terminal as a passthrough for an unmanaged peripheral's data was the natural, predictable approach. EX1003, ¶32.

D. Transmitting Multiple Types of Data Over an Established Communication Session Was Well-Known

Moreover, combining camera video and shared content within a single session was well understood. EX1003, ¶33. Comstock's system simultaneously handles "people" and "content" streams, combining them through a single multiplexer and network communication stack. EX1008, FIG.2, 5:20-8:31. Toya transmits both real-time participant video and supplemental content data over the same established

call session. EX1004, FIGS. 14-16, 29:28-31:12. U.S. Patent Application Publication No. 2012/0133727 (Bolduc) describes a presenter device that captures both camera video and screen content, sends both to a streaming server, and the server rebroadcasts them to attendees. EX1012, Abstract, FIG1, 4A/4B. Multiplexing camera video and shared content over a conferencing session was well known. EX1003, ¶33.



EX1004, FIG16.

E. Transmitting Programs to Connected Peripheral Devices Upon Connection, with Conditional Installation, Was Well-Known

The specific interaction pattern—in which a host device receives a request from a connected peripheral, grants permission, transmits a program to the peripheral if not already installed, and receives data captured by the program executing on the peripheral—was a thoroughly documented and widely deployed technique in the connected-device ecosystem years before the '917 Patent's priority date. EX1003, ¶34.

The USB Plug-and-Play architecture, which was standardized and ubiquitous well before 2010, established a paradigm for host-peripheral program exchange. EX1003, ¶35. U.S. Patent No. 7,668,986 describes a peripheral device that, upon connection to a host, initially presents itself as a mass storage device to permit the host to access and install driver software stored in the peripheral's memory, and then transitions to a second mode enabling full device functionality once the drivers are installed. EX1013, Abstract; FIGS1-2. Lowe teaches that the peripheral device stores its own drivers internally and that the host checks whether an appropriate driver already exists before performing installation—the same conditional-installation logic recited in claim 6. EX1003, ¶35.

SMART Technologies ULC's U.S. Patent No. 8,190,785 (Hill) discloses a “plug-and-play” peripheral device comprising a cable with embedded storage that

stores driver software. EX1014, Abstract. When the peripheral is connected to a host computer, the host detects the peripheral, determines whether appropriate driver software is already installed, and if not, retrieves and installs the driver from the peripheral's embedded storage to enable the host to access the peripheral's data-capture functionality. EX1014, Abstract, FIG1, 1:8-2:11, 3:55-4:46. Thus, the pattern of checking for existing software before transmitting and installing a program from a host-connected device was well-known by 2006. EX1003, ¶36.

Marvell's U.S. Patent No. 8,260,978 (Thompson) describes a host device that detects a peripheral device, determines whether a driver is already installed, and if not, executes the auto-installation program retrieved from the peripheral to install the necessary software enabling the host to communicate with the peripheral. EX1015, Abstract, FIGS1-4, 2:66-4:45. This teaches the conditional-installation check—the host evaluates whether existing software on the host already supports the peripheral before initiating installation—was well known. EX1003, ¶37.

SMART Technologies ULC's International Publication No. WO 2010/105335 (Banerjee) describes a plug-and-play device comprising storage that stores "code that is automatically executed by the . . . computing device when said plug-and-play device is connected thereto," with the code "when executed initiating a screen display data exchange" between computing devices. EX1016, [0009],

[0003]. Thus, transmitting a program from a device to a connected host (or vice versa) upon connection, with conditional installation, was a standard plug-and-play design pattern for enabling screen data exchange between devices. EX1003, ¶38.

These references collectively establish that by 2008—well before the '917 Patent's priority date—the claimed interaction pattern was well-known in the art of connected-device software deployment. EX1003, ¶39. Specifically, the prior art demonstrates that it was known for a host device to: (a) detect when a peripheral is connected and receive a request or notification that initiates a software interaction; (b) determine whether the necessary program is already installed on the peripheral or host; (c) transmit the program to the device that lacks it if it is not already present; and (d) upon successful installation and permission, execute the program to acquire data from the device. EX1003, ¶39.

III. '917 PATENT

A. Overview

The alleged invention of the '917 Patent relates to nothing more than (1) a first transmission terminal logging into a management system and establishing a communication session for a video conference with a second transmission terminal that has also logged into the management system, (2) receiving display data from an external input apparatus (such as a laptop computer) that has *not* logged into the management system when that apparatus is connected to the first transmission

terminal during the video conference, and (3) forwarding the received display data—along with the first terminal’s own video data—to the second transmission terminal using the already-established communication session. *See* EX1001, claims 1, 8, 15; EX1003, ¶40.

But this alleged invention was well-known in the art. The ’917 Patent concedes that conducting video conferences by transmitting video and audio data between plural transmission terminals over a communication network was already commonplace, and that it was separately known to transmit “presentation content” alongside audio and video data to conference participants. *See* EX1001, 1:40-2:3. The only purported distinction is that the external input apparatus need not itself log into the transmission managing system because the first terminal—already authenticated and in session—acts as a conduit for the external apparatus’s display data, relaying it through the same relay apparatus that carries the video conference traffic. *See* EX1001, 2:15-21, 28:60-29:10; EX1003, ¶41.

Thus, the ’917 Patent describes nothing more than the trivial step of forwarding screen-share data from an unmanaged device through a terminal that is already participating in a video conference session—a concept that merely combines the well-known functions of receiving data from a connected peripheral and transmitting that data over a pre-existing communication path. *See* EX1001, 28:60-29:10. The substance of the claims adds nothing beyond what a person of ordinary

skill would have understood as the application of known data-forwarding techniques in the video conferencing context. EX1003, ¶42.

B. Prosecution History

The application that issued as the '917 Patent (Application No. 16/589,700) was filed on October 1, 2019, with a single independent claim. EX1002, Filing Receipt; EX1003, ¶43.

The Office issued a first non-final office action on March 5, 2020, rejecting claim 1 under 35 U.S.C. §103 as being unpatentable over Saito et al. (U.S. Pub. No. 2005/0060547) in view of Ikeda et al. (U.S. Patent No. 8,400,530). EX1002, 167-171. The Examiner also rejected claim 1 on the ground of nonstatutory double patenting as being unpatentable over claims 1–8 of U.S. Patent No. 9,787,944 and over claims 1–8 of U.S. Patent No. 10,178,349. EX1002, 171-173; EX1003, ¶44.

In response, on June 5, 2020, Applicant amended claim 1 and added new claims 2–15 (including new independent claims 8 and 15). EX1002, 186-191. The amendments added limitations requiring that the first transmission terminal “log into a management system by transmitting a login request to the management system,” “establish a communication session for transmitting the first video data to a second transmission terminal that has logged into the management system,” and receive second video data from “an external input apparatus that has not logged into the management system.” EX1002, 186. Applicant argued that the amended claims

patentably distinguished over Saito and Ikeda because neither reference taught these features. EX1002, 192-194; EX1003, ¶45.

The Examiner issued a final office action on August 6, 2020, finding claims 1–15 allowable over the prior art of record but maintaining a rejection on the ground of nonstatutory double patenting as being unpatentable over claims 1–13 of U.S. Patent No. 10,477,147. EX1002, 201-205; EX1003, ¶46.

On September 21, 2020, Applicant submitted a terminal disclaimer to overcome the double patenting rejection. EX1002, 216-219; EX1003, ¶47.

On October 21, 2020, the Examiner issued a Notice of Allowance for claims 1–15, accepting the terminal disclaimer and finding the claims allowable. EX1002, 233-243. In the Examiner’s Statement of Reasons for Allowance, the Examiner noted that updated searches identified several references—including Kato et al. (US 2019/0107988), Kagawa (US 2020/0273464), Shiro et al. (US 2018/0041553), Homma et al. (US 2018/0027030), Horiuchi et al. (US 2017/0264450), and Umehara et al. (US 2016/0150023)—but found none that taught all features of the amended independent claims. EX1002, 233-234, 239-240; EX1003, ¶48.

On January 7, 2021, Applicant filed an amendment after allowance under 37 C.F.R. §1.312 to clarify claim language and correct terminology. EX1002, 252-258. The Examiner entered the amendment on January 14, 2021. EX1002, 268-270; EX1003, ¶49.

As demonstrated by the grounds of this Petition, the added claim limitations used to distinguish the claims from Saito and Ikeda—requiring login to a management system, establishing a session with a second terminal that has logged in, and receiving data from an external apparatus that has not logged in—were well-known, as were the Challenged Claims as a whole. The Examiner never had the opportunity to evaluate the Challenged Claims in light of the Toya, Tucker, U.S. Patent No. 8,316,138 (Chang), and RFC 3261 references and their combinations presented herein; EX1003, ¶50.

IV. POSITA

A person of ordinary skill in the art (“POSITA”) relevant to the ’917 Patent as of May 6, 2010 would have had at least: (1) a bachelor’s degree in electrical engineering, computer science, computer engineering, or equivalent coursework, with at least two years of work experience in video communication systems, networked multimedia applications, or conferencing system architectures; or (2) a master’s degree in electrical engineering, computer science, computer engineering, or equivalent coursework, with coursework or research focused on video conferencing systems, real-time media transmission, or networked communication protocols. An individual with additional education could have less practical experience, and vice versa. EX1003, ¶51.

V. CLAIM CONSTRUCTION

Petitioner contends that no express constructions are necessary for determining whether the prior art teaches or renders obvious every limitation of the Challenged Claims. EX1003, ¶52.

VI. OVERVIEW OF CHALLENGE

Petitioner requests cancellation of claims 1-15 as set forth below:

Ground	Claims	Statutory Basis	References
1	1-3, 7-10, 14-15	§103	Toya in view of Tucker
2	4-6, 11-13	§103	Toya in view of Tucker in further view of Chang
3	1-3, 8-10, 15	§103	Toya in view of RFC 3261
4	4-6, 11-13	§103	Toya in view of RFC 3261 in further view of Chang

The application that issued as the '917 Patent was filed on October 1, 2019, and is a continuation of an application filed on November 15, 2018, which traces through a chain of continuations to International Application No. PCT/JP2011/060676, filed April 27, 2011, which claims priority to Japanese Application No. 2010-106610, filed May 6, 2010. Petitioner's challenge is based on the following references, which are prior art under 35 U.S.C. §102 (pre-AIA). None of these references were considered or cited during prosecution of the '917 Patent.

Exhibit	Reference	Date(s)	Availability as Prior Art
EX1004	U.S. Patent No. 8,305,422 ("Toya")	Filed Jul. 9, 2008; Issued Nov. 6, 2012	§§102(a), 102(e)

EX1005	U.S. Patent Application Publication No. 2010/0066805 (“Tucker”)	Published Mar. 18, 2010	§§102(a), 102(b)
EX1006	RFC 3261	Published June 2002	§102(b)
EX1007	U.S. Patent No. 8,316,138 (“Chang”)	Filed Sep. 7, 2010 (priority Nov. 24, 2006); Issued Nov. 20, 2012	§102(e)

VII. THE ASSERTED GROUNDS OF INVALIDITY

A. Ground 1: Toya in view of Tucker Renders Obvious Claims 1-3, 7-10, 14-15

Toya in view of Tucker renders obvious every limitation of claims 1-3, 7-10, 14-15. Toya provides the foundational video conferencing architecture in which a communication device establishes a call session with another device, captures and transmits video data, receives content data from an external source, and forwards that content to the other device over the established session. Toya does not provide details on the mechanism by which terminals are authorized for use of the system. A POSITA would have understood that in a real-world system, for example, a commercial version of Toya, some form of authorization and authentication would be necessary. Tucker supplies the details of how terminals log into a centralized management system by transmitting a login request before establishing the communication session by disclosing a server-mediated video conferencing system in which a remote user is authenticated through a website before the video

conference is initiated, including accessing a user database to verify the user's authorization and establishing the session only upon successful verification. EX1003, ¶55.

1. Motivation to Combine

A POSITA would have been motivated to incorporate Tucker's server-based user authentication into Toya's SIP-based video conferencing and content-sharing system for several independently sufficient reasons. EX1003, ¶[56].

Same Field of Endeavor: Toya and Tucker are in the same field of endeavor: both are directed to video conferencing systems that establish sessions between remote participants and transmit video data over a communication network. EX1003, ¶[57]. Toya discloses a "video communication device" that "function[s] as a television conference system terminal device" and establishes "a call session with another video communication device serving as a counterpart device, thereby realizing reception and transmission of video data and audio data therebetween." EX1004, 16:51-64. Tucker likewise discloses a system and method "for implementing a video conference through a television forwarding device" or set-top box in which a remote user and a local user exchange video conference signals. EX1005, ¶¶[0003], [0059], Abstract. Both references address how to manage the initiation and conduct of video conferences between networked

endpoints. A POSITA designing a video conferencing system with content-sharing capabilities would have naturally looked to both references. EX1003, ¶[57].

Tucker Solves a Problem That Toya's System Faces: Toya's system faces a fundamental security and access-control necessity that Toya does not focus on: how to ensure that only authorized users can initiate or participate in video conference sessions. EX1003, ¶[58]. Toya discloses that its video communication device establishes call sessions using SIP signaling, but Toya does not address the details of a mechanism for verifying the identity or authorization of the terminals before permitting the session to proceed. EX1004, 16:65-17:26. Without an authentication mechanism, any device with network access could potentially initiate a call session with Toya's video communication device, raising obvious concerns about unauthorized access and misuse. EX1003, ¶[58]. Tucker directly solves this necessity. Tucker expressly teaches "authenticating a remote user through a website" before permitting the video conference to be implemented, including "accessing a user database to determine that the remote user is authorized to communicate with the television forwarding device" or set-top box and "verifying an identifier received from the remote user." EX1005, claims 1, 13, [0003], [0021]-[0023], [0053]-[0054],[0059]-[0061], FIG4. A POSITA would have been motivated to incorporate Tucker's pre-session authentication into Toya's conferencing system to restrict conference participation to authorized users and prevent unauthorized access—a

universally recognized security objective in networked communication systems. EX1003, ¶[59].

Tucker Ensures Only Authorized Users Communicate: A POSITA would have been well aware and Tucker confirms the need for requiring authentication before initiating a video conference. EX1003, ¶[60]. Tucker teaches that the system includes “a database in communication with the server, the database configured to verify that the remote user is authorized to communicate with the television forwarding device.” EX1005, claim 15, [0023]. Tucker further teaches encrypting and decrypting the video conference using digital rights management keys, confirming that controlling access to conferencing sessions was a central design objective. EX1005, claim 16, [0022]-[0024]. This same concern applies directly to Toya’s system: without authentication, Toya’s content-sharing functionality—which automatically forwards externally obtained content data to the conferencing counterpart—could be exploited by unauthorized users. EX1003, ¶[60]. A POSITA would have recognized that incorporating Tucker’s authentication step into Toya’s system would address this concern, ensuring that content is shared only with verified, authorized participants. EX1003, ¶[60].

Predictable Combination of Known Elements: The combination of Toya and Tucker is the predictable use of known prior art elements according to known methods to yield predictable results. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398,

415-421 (2007). Toya teaches a video conferencing terminal that establishes SIP-based call sessions, transmits camera video to a counterpart device, receives content data from external sources, and forwards that content to the counterpart over the established session. EX1004, 16:51-17:43, 18:24-49, 20:23-32. Tucker teaches a centralized server that authenticates users by verifying credentials against a user database before permitting a video conference to proceed. EX1005, claims 1, 13, 15, [0022]-[0024]. Incorporating Tucker's pre-session authentication step into Toya's system yields the entirely predictable result: before Toya's video communication device establishes a SIP call session with a counterpart device, both devices first authenticate with a centralized server, and the session proceeds only upon successful verification. EX1003, ¶[61]. The underlying video conferencing, content acquisition, and content forwarding functions disclosed by Toya remain unchanged; the only modification is the addition of an authentication prerequisite before session establishment. EX1003, ¶[61].

Using a Known Technique to Improve a Similar Device in the Same Way: The combination is further supported under *KSR* as using a known technique (Tucker's server-based user authentication via username/password verification against a user database) to improve a similar device (Toya's SIP-based video conferencing terminal with content-sharing capabilities) in the same way (restricting conference participation to authenticated users before permitting session

establishment). *KSR*, 550 U.S. at 417. A POSITA would have had a reasonable expectation of success because Toya's system already uses network-based signaling protocols (SIP) to establish call sessions, and adding a pre-session authentication exchange with a centralized server—as taught by Tucker—would have been a straightforward modification requiring the addition of a credential-verification step prior to the SIP INVITE message. EX1003, ¶¶[62]-[63]. SIP-based systems were well-known to support integration with authentication servers and registrars, and a POSITA would have understood that pairing Toya's SIP signaling with Tucker's server-based authentication was a routine engineering task well within ordinary skill. EX1003, ¶[64].

The External Input Apparatus Remains Unauthenticated: Importantly, the combination preserves Toya's architecture in which the external content source (e.g., a mobile phone connected via a wired or wireless connection) does not participate in the conferencing session and does not authenticate with the management server. EX1003, ¶[65]. In the combined system, only the video communication devices (transmission terminals) that participate in the call session authenticate with Tucker's server; the external device that supplies content data to the authenticated terminal through a local interface is not required to log in. EX1003, ¶[65]. This is the precise configuration recited in the '917 Patent's claims, which require that the external input apparatus “has not logged into the management

system.” EX1001, claim 1. The combination thus naturally and predictably arrives at the claimed architecture without any non-obvious modification. EX1003, ¶[66].

2. Preambles

a) [1.pre]

Toya discloses this element. Toya describes a “video communication device 1” that functions as “a television conference system terminal device.” EX1004, 16:42-57. The video communication device 1 includes a CPU 20, ROM 21, and RAM 22, which collectively constitute processing circuitry that executes a program to control the device’s communication, content acquisition, and content transmission functions. EX1004, 16:35-57, 21:64-22:32; FIG1, 3. The CPU 20 functions as the communication control section 2, the communication processing section 3, the communication input section 4, and the communication output section 5, as well as the content receiving section 6, the content storage section 7, and the content transmission section 8. EX1004, 16:42-17:10; 22:3-10; FIG1, 3. A POSITA would have understood that Toya’s **video communication device 1, with its CPU-based processing architecture**, constitutes a “first transmission terminal comprising processing circuitry.” EX1003, ¶[67].

FIG. 3

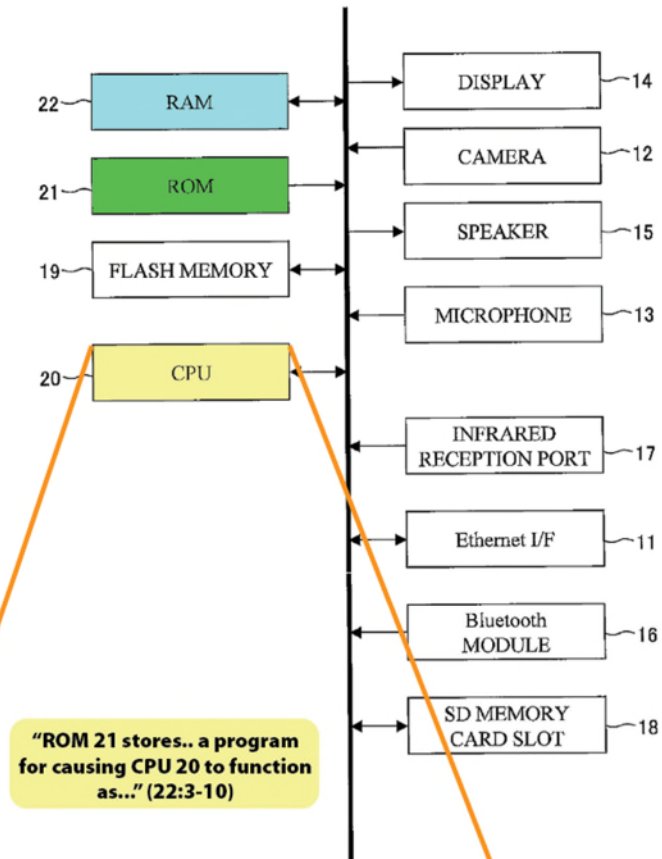
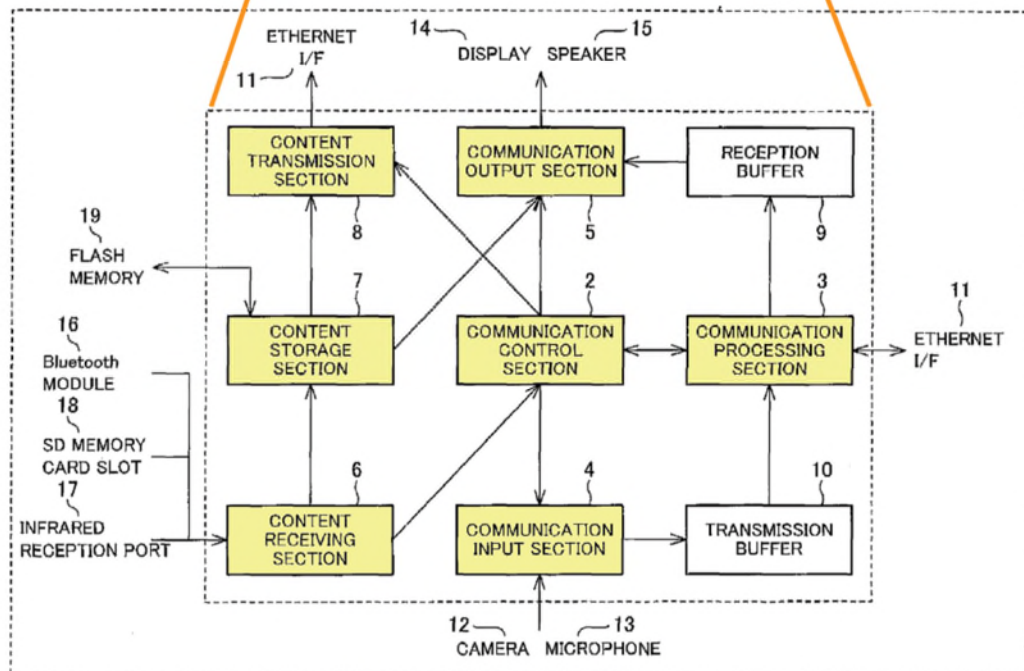


FIG. 1



b) [8.pre]

Toya discloses performing the method of claim 8. Toya's video communication device 1, when executing the software stored in its ROM 21 and controlled by its CPU 20, performs the functional operations of establishing a call session via SIP signaling, capturing and transmitting video data through its camera 12 and communication processing section 3, receiving content data from an external device through its content receiving section 6, and transmitting the received content data to the counterpart device through its content transmission section 8. EX1004, 16:35-17:26, 17:58-18:41 20:6-32, 21:64-22:10., FIGS. 9, 14-16. A POSITA would have understood that any processor-based system that performs functional operations through software execution necessarily performs the steps of a method. EX1003, ¶[68]. The execution of video conferencing software by Toya's CPU 20 to control call session establishment, video capture and transmission, content acquisition from external devices, and content forwarding to the counterpart device constitutes performance of a method. EX1003, ¶[68].

Tucker likewise discloses performing a method. Tucker's claims "[a] method for implementing a video conference through a television forwarding device, the method comprising: authenticating a remote user through a website; receiving a selection of a user for the remote user to communicate with through the video conference; sending an invitation to the television forwarding device ... and

implementing the video conference between the remote user and the user in response to the user accepting the invitation.” EX1005, claim 1, [0003]. Tucker’s authentication process—in which a user submits credentials through a website and the server accesses a user database to verify authorization—is performed as method steps by the server and the user’s communications device. EX1005, claims 1, 13, [0022]-[0023], [0061]; EX1003, ¶[69].

In the combination, Toya’s CPU 20 executes the method steps of obtaining first video data from the camera, establishing a call session with a counterpart device, transmitting the video data over the session, receiving content data from an external device, and transmitting both the video data and the content data to the counterpart device—while Tucker’s server performs the method step of authenticating the terminals before the session is established. EX1003, ¶[70]. The combination of Toya and Tucker thus renders obvious every method step recited in claim 8 for the same reasons discussed with respect to the corresponding limitations of claim 1. EX1003, ¶[70].

c) [15.pre]

Toya discloses a non-transitory computer readable medium storing computer-executable instructions. Toya describes that its video communication device 1 includes a ROM 21 and a flash memory 19, both of which store programs and data for controlling the device’s operations. EX1004, 21:64-22:32, FIG1, 3. Toya further

discloses that the video communication device 1 includes a CPU 20 that executes the programs stored in the ROM 21 and flash memory 19, causing the device to perform the conferencing, content acquisition, and content transmission functions described above. *Id.* The ROM 21 and flash memory 19—which are non-volatile storage media retaining the program instructions even when the device is powered off—constitute “non-transitory computer readable medium[s]” within the meaning of claim 15. EX1003, ¶[71].

Toya also discloses that its invention may be embodied in a computer-readable storage medium. Toya claims “a non-transitory computer-readable storage medium, storing therein a program for causing a computer to function as the means of the communication device.” EX1004, claim 17. This further confirms that Toya contemplated embodying its conferencing and content-sharing functionality as stored program instructions on a non-transitory medium. EX1003, ¶[72].

Tucker likewise discloses stored program instructions. Tucker’s server stores program logic that implements the authentication, invitation, and video conference management functions, and the television forwarding device or set-top box includes “video conference logic” operable to control video conferencing operations. EX1005, ¶¶[0004]-[0005],[0065]. In Tucker’s embodiments, this server (e.g., communications management system 112 or 404) handles routing and management of video communications between communications devices, as well as

authentication of users. EX1005, ¶¶ [0019], [0022]. In the combination, the authentication step taught by Tucker would be implemented as stored instructions executed by Toya's CPU 20, alongside the existing conferencing and content-sharing instructions already stored in Toya's ROM 21 and flash memory 19. EX1003, ¶[73].

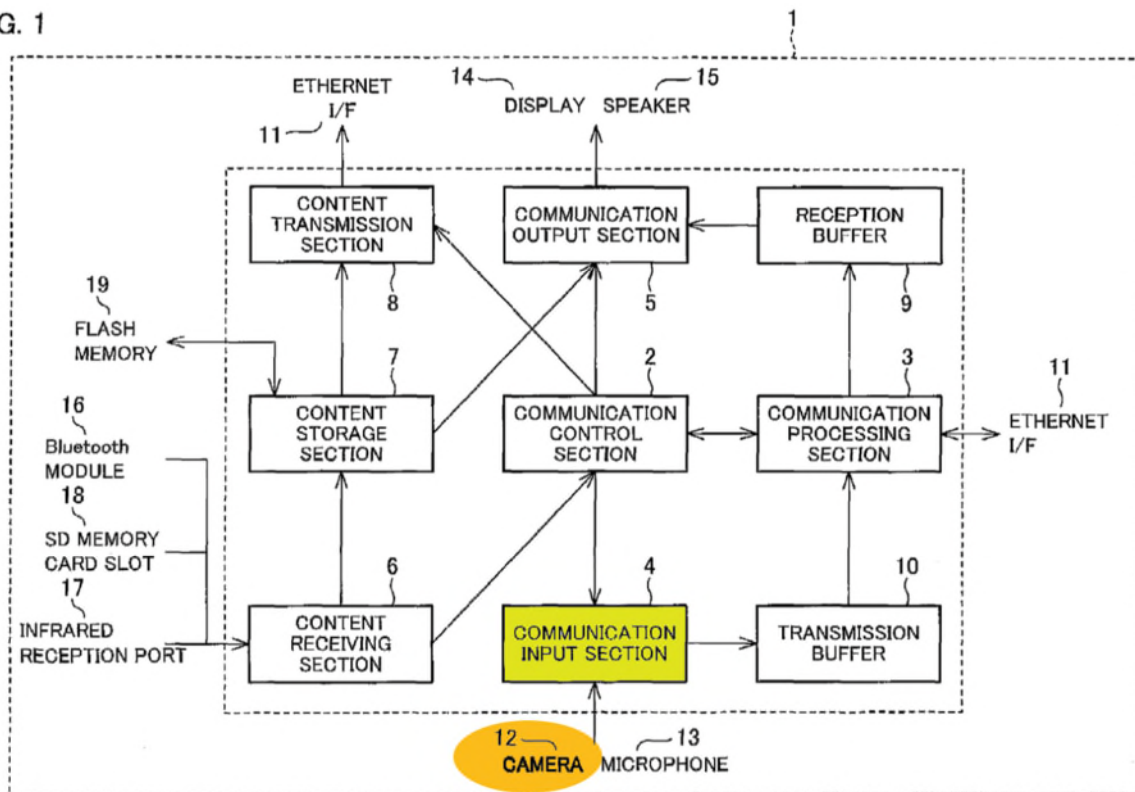
The stored instructions in Toya's non-transitory medium, as modified by Tucker's authentication teachings, when executed by Toya's CPU 20, cause the video communication device 1 to perform the same operations described in the claim 1 analysis: obtaining video data from the camera, logging into the management system, establishing a communication session with an authenticated counterpart, transmitting video data, receiving content data from an external device that has not logged into the management system, and transmitting both the video data and the content data for sharing with the counterpart using the established session. The combination of Toya and Tucker thus renders obvious every limitation of claim 15 for the same reasons discussed with respect to the corresponding limitations of claim 1. EX1003, ¶[74].

3. [1.a]/[8.a]/[15.a]

Toya discloses this element. Toya's video communication device 1 includes a communication input section 4 comprising a camera 12 and a microphone 13. EX1004, 18:3-11; FIG1. The **camera 12** captures video data of the local user, and

the communication input section 4 provides this captured video data for transmission to a counterpart device during a television conference call session. EX1004, 17:11-26. The captured video data from the camera constitutes the claimed “first video data captured by a camera.” EX1003, ¶¶ [75]-[77].

FIG. 1



4. [1.b]/[8.b]/[15.b]

Toya does not explicitly disclose logging into a management system by transmitting a login request. Tucker discloses this element.

Tucker teaches a video conferencing system in which a user must be “authenticated through a website” before initiating or participating in a video conference. EX1005, ¶[0003], Abstract claim 1, 5. Tucker’s authentication process

involves “accessing a user database to determine that the remote user is authorized to communicate with the television forwarding device” or set-top box and “verifying an identifier received from the remote user.” EX1005, claim 13, [0022]-[0023], [0053]-[0054], [0059]-[0061]. As illustrated in Tucker’s FIG. 6, the user submits a username and password through a graphical user interface to initiate the video conference, and the system verifies those credentials before permitting the session to proceed. EX1005, FIG6, FIG7, ¶¶[0054], [0060]-[0065], [0071]-[0072], [0077]. **The submission of a username and password to the server for verification constitutes “transmitting a login request to the management system,” and the server that hosts the website, stores the user database, and performs the authentication constitutes the claimed “management system.”** EX1003, ¶¶ [78]-[79]. Tucker further discloses that this server functionality may be embodied as communications management system 112 or 404, which may include any number of servers to authenticate remote users. EX1005, ¶¶[0019],[0022].

FIG. 6

600

Step 1: Initiate Video Conference

Username: CTucker

Password: *****

☒ Configure User Preferences

602

Step 2: Select Participant(s)

Network Address Book 608

☐ Work

☒ Home

☐ Mom and dad

☐ Guest House

604

Step 3: Select Resolution

Highest 704x480(4CIF)

Medium High 704x240(2CIF)

Medium Low 352x240(CIF)

Low 176x120(QCIF)

606

Step 4: Start/Stop

Initiate Video Conference

End video conference

608

FIG. 7

Graphical User Interface 700

Accept incoming video conference from Mike31?

☐ Y ☐ N

Begin video conference call?

☐ Y ☐ N

Username: Jesse

Password: *****

Select recipient(s): ▼

Select bandwidth: ▼

End video conference call?

XXX

☐ Y ☐ N

In the combination, Toya's video communication device 1 would be modified to authenticate with a centralized server (as taught by Tucker, (e.g., 112 or 404)) before establishing a call session with a counterpart device. EX1003, ¶[80]. A POSITA would have understood this to be a predictable addition of a well-known pre-session authentication step to Toya's existing SIP-based conferencing architecture. EX1003, ¶¶[80]-[81].

5. [1.c]/[8.c]/[15.c]

The combination of Toya and Tucker teaches this element.

Toya discloses that “the communication control section 2 controls the communication processing section 3, the communication input section 4, and the communication output section 5, and establishes a call session with another video communication device serving as a counterpart device, thereby realizing reception and transmission of video data and audio data therebetween.” EX1004, 16:58-64. The establishment of the call session is “realized by controlling ‘call control signaling’ between the video communication device 1 and the counterpart device which carry out communication call with use of SIP.” EX1004, 16:65-17:2. The counterpart device is itself a video communication device of the same type, capable of performing the same functions. EX1004, FIG9. **The call session established between the two devices constitutes the claimed “communication session for**

transmitting the first video data to a second transmission terminal.” EX1003, ¶¶ [82]-[83].

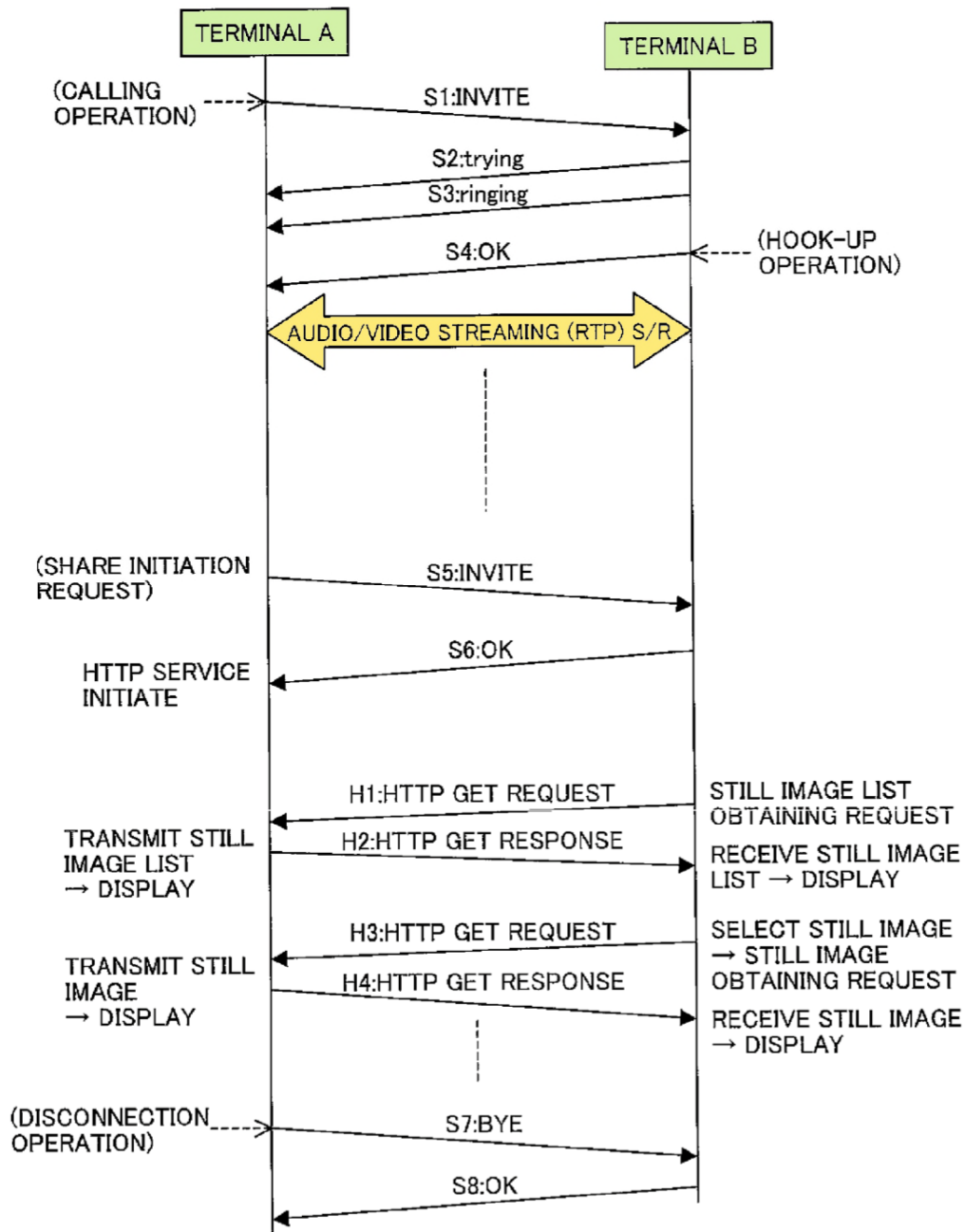
Tucker supplies the requirement that the second terminal “has logged into the management system.” EX1003, ¶[84]. In Tucker’s system, both participants must be authenticated before the video conference is implemented. EX1005, ¶[0003], [0022]-[0023], [0053]-[0054], claims 1, 13-15. The server (e.g., Tucker’s communications management system 112 or 404) verifies that both the remote user and the local user are authorized to communicate before permitting the session. EX1005, [0004], [0022]-[0023], [0053], [0061], claim 15. In the combination, both Toya’s first and second video communication devices would authenticate with the management server before the SIP call session is established, satisfying this limitation. EX1003, ¶¶ [84]-[85].

6. [1.d]/[8.d]/[15.d]

Toya discloses this element. Once the call session is established, Toya’s video communication device 1 transmits video data captured by the camera 12 and audio data captured by the microphone 13 to the counterpart device via the communication processing section 3. EX1004, 16:51-18:11, 26:39-43; FIG1, FIG9 (showing bidirectional audio/video streaming transmission between terminal A and terminal B during the call session). The transmission of this camera-captured video data over

the SIP-based call session constitutes “transmit[ing] the first video data using the established communication session.” EX1003, ¶¶ [86]-[88].

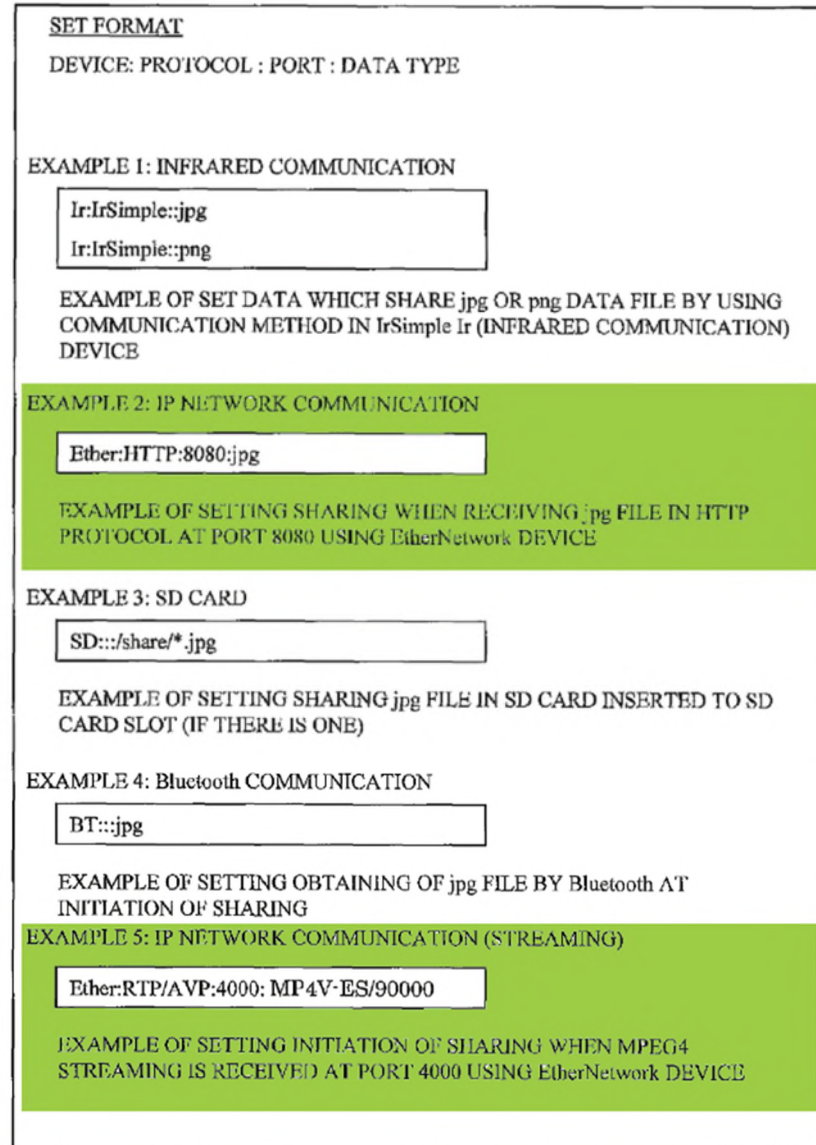
FIG. 9



7. [1.e]/[8.e]/[15.e]

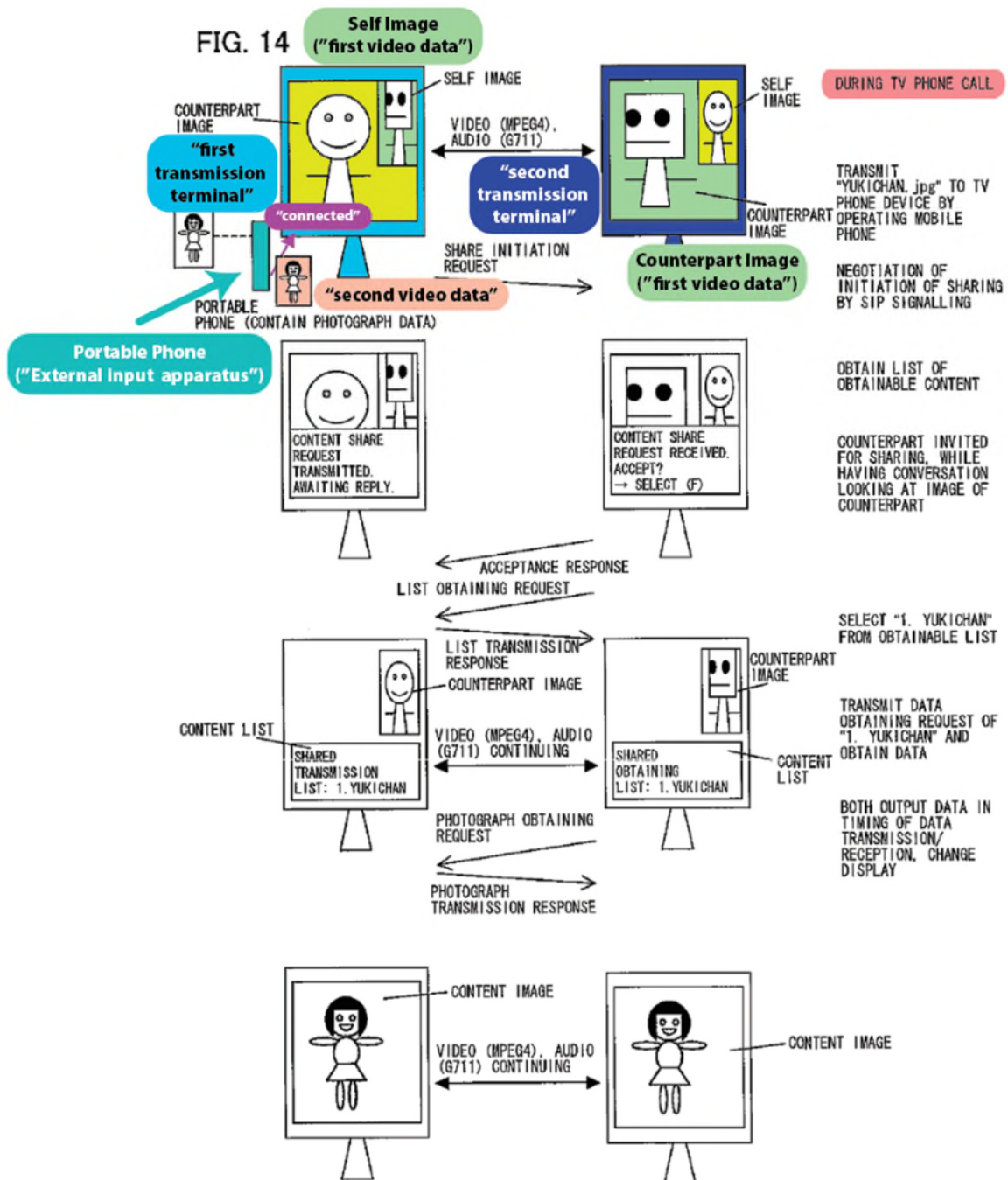
The combination of Toya and Tucker teaches this element. Toya discloses that the video communication device 1 includes a content receiving section 6 that is “arranged so as to obtain content data from the outside of the video communication device 1.” EX1004, 18:24-41. The video communication device 1 includes “a plurality of interfaces for receiving data from the outside,” including “an infrared reception port 17 and a Bluetooth (registered trademark) module 16 as communication devices for receiving data from an external device,” as well as “an SD memory card reader 18 as a reproduction device for reading out data from the storage medium” and an “**Ethernet I/F 11.**” EX1004, 18:32-59. FIG. 8, examples 2 and 5 demonstrate the wired connections between the external input apparatus and the first transmission terminal. “Example 2 is a content data set received at an HTTP protocol from a port 8080 via the Ethernet I/F 11.” EX1004, 26:2-3. And, “example 5 shows the setting for sharing an MPEG4 data stream received at a port 4000 via the Ethernet I/F 11.” EX1004, 26:10-11; EX1003, ¶¶ [89]-[90].

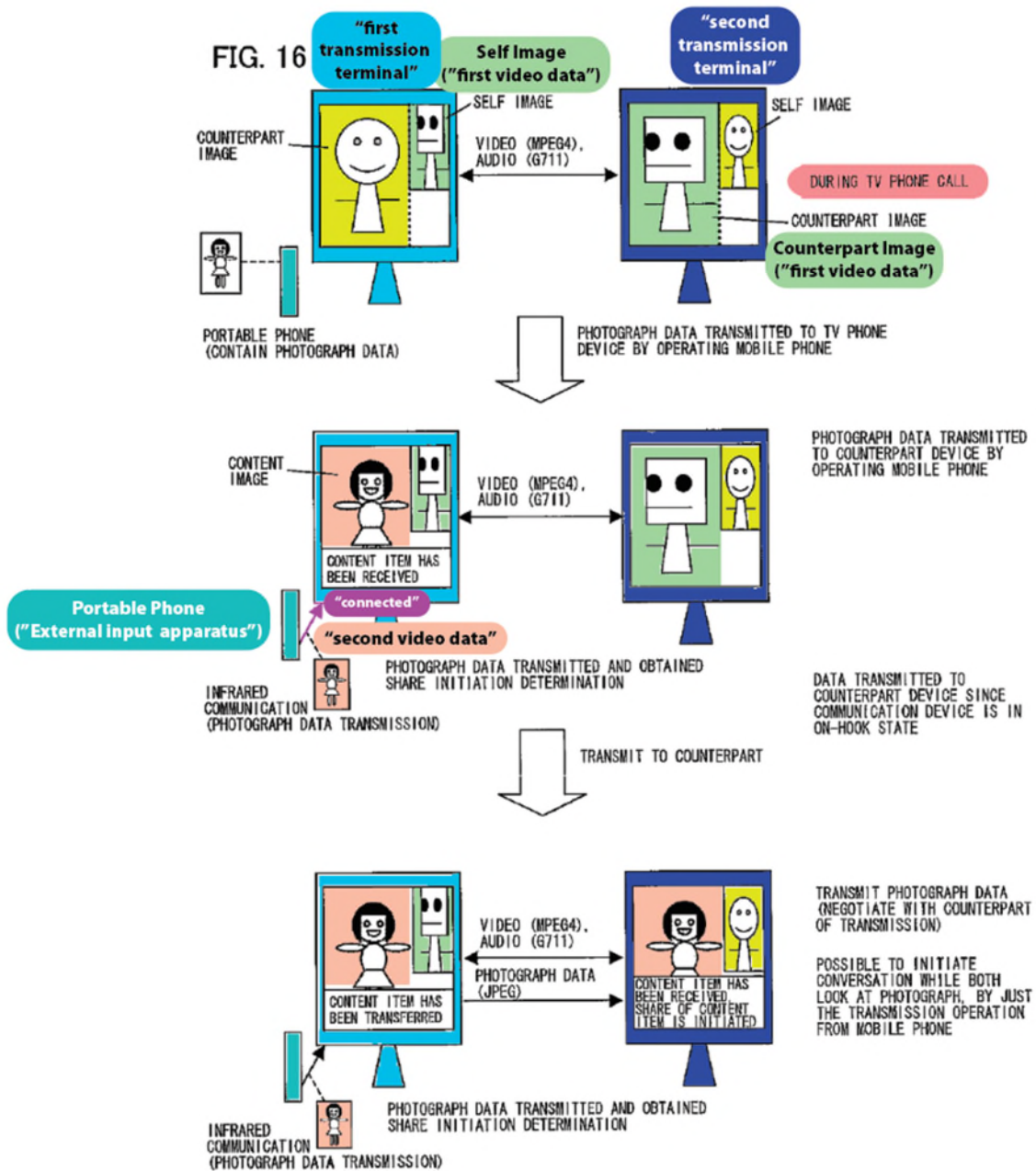
FIG. 8



External devices such as a mobile phone transmit content data (including photograph data and video data) to the video communication device 1 via these interfaces. EX1004, FIG14-16, 24:50-56, 29:34-31:12. The content data obtained from these external sources constitutes the claimed “second video data obtained in the external input apparatus.” EX1003, ¶[91].

Toya further discloses that the content data is received from the external device *during an ongoing call session* in which the video communication device 1 is already transmitting video data to the counterpart device and the counterpart device is displaying the video conference on its display. EX1004, FIGS. 14-16 (showing content sharing occurring during an active television phone call). The external device (e.g., the mobile phone) has not established its own call session with the counterpart device and is not a participant in the conferencing system; it merely sends data to the video communication device 1 through a local interface. EX1004, 18:32-49, 24:50-56, 29:34-31:12, FIG14-16. EX1003, ¶[92].





Combining with Tucker is consistent with the requirement that the external input apparatus “has not logged into the management system.” EX1003, ¶[93]. In the combination, the management system authenticates only the video communication devices (transmission terminals) that participate in the conference,

not the external devices (such as mobile phones or SD cards) that supply content data to those terminals through local interfaces. EX1003, ¶[93]. A POSITA would have understood that Toya's external mobile phone or other content source—which connects locally to the video communication device via Bluetooth, infrared, SD card or Ethernet I/F—would not separately authenticate with Tucker's management server, because the external device does not participate in the conferencing session; it merely supplies data to the authenticated terminal. EX1003, ¶[93]. Moreover, Toya already provides security relating to its external device connection, which does not include logging in. EX1004, 27:52-28:2. Thus, a POSITA would understand that the combination of Tucker with Toya would not require (and Toya teaches against) the external device logging into the management system. EX1003, ¶¶[93]-[94].

8. [1.f]/[8.f]/[15.f]

Toya discloses this element. Toya discloses that when the content receiving section 6 obtains content data from an external device, the content transmission section 8 “specif[ies] another communication device as a communication device, to which the obtained content data should be transmitted, if connection with said another communication device is established when the content receiving section (6) obtains the content data.” EX1004, Abstract. The content transmission section 8 transmits the obtained content data to the counterpart device over the established call

session. EX1004, 18:24-31, 19:28-43, 20:23-41. During this process, the video communication device 1 continues to transmit its own camera video data and audio data to the counterpart device. EX1004, FIGS. 14-16 (showing “VIDEO (MPEG4), AUDIO (G.711)” continuing alongside “PHOTOGRAPH DATA (JPEG)” transmission). As illustrated in Toya’s FIG16, the counterpart device displays both the conference video and the shared content data simultaneously, with the “SELF IMAGE,” “COUNTERPART IMAGE,” and “CONTENT IMAGE” all appearing on the display. EX1004, FIG16. EX1003, ¶¶[95]-[96].

Thus, in response to receiving the content data from the external device, Toya’s video communication device transmits both the first video data (camera video) and the second video data (content from the external device) for sharing with the counterpart device using the established call session. EX1003, ¶[97]. This satisfies the claim requirement of transmitting “the first video data and the second video data for sharing with the second transmission terminal using the established communication session.” EX1003, ¶¶ [97]-[98].

9. Claim 2/9

Toya in view of Tucker renders obvious claim 2. EX1003, ¶[99]. Claim 2 depends from claim 1 and further requires that “the processing circuitry is configured to transmit the first video data and the second video data via a relay apparatus.” EX1003, ¶¶ [99]-[100]

Toya discloses the use of SIP and internet protocol networking, which inherently involves the relaying of information from device to device across the network, for example via IP switches, hubs, and routers. EX1003, ¶[100]. The SIP headers disclosed in Toya expressly acknowledge this by specifying “max-forwards” parameters, which specify the maximum number of hops (i.e., relays) that the message is permitted to take between source and destination. EX1003, ¶[101]; EX1004, FIG10, FIG13, FIG17.

FIG. 13

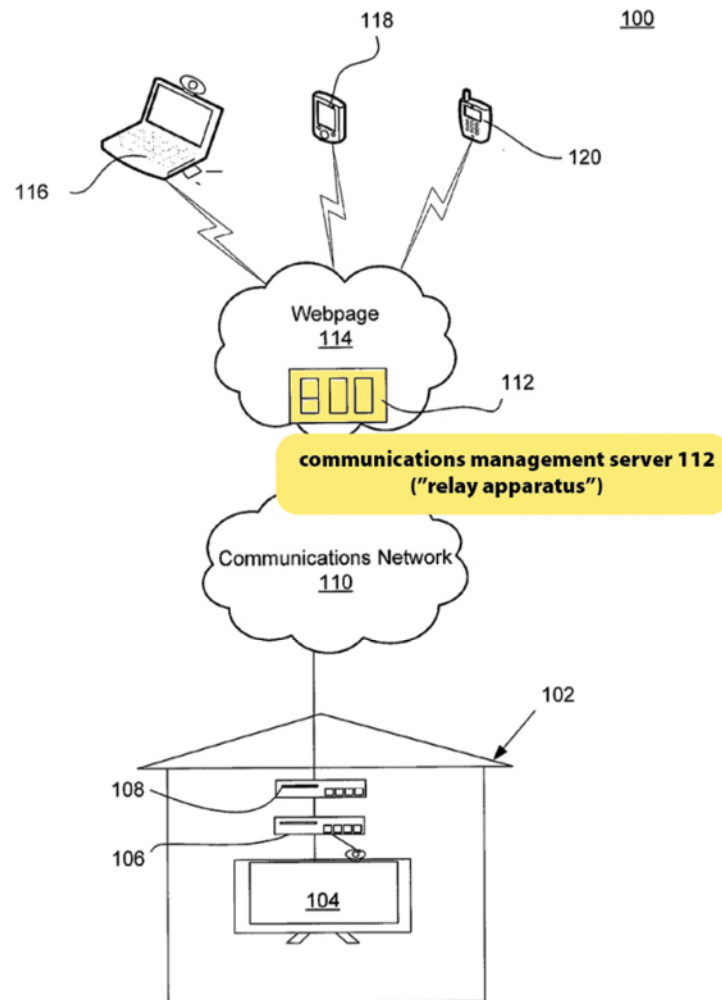
```
INVITE sip:vc2@vc.sharp.co.jp SIP/2.0
Via: SIP/2.0/UDP 172.16.0.163:5060;branch=z9hG4bK1066896417
From: "Mari" <sip:vc1@vc.sharp.co.jp>;tag=897334059-1-0
To: <sip:vc2@vc.sharp.co.jp>;
Call-ID: 1365018947@172.16.0.163
CSeq: 2 INVITE
Contact: <sip:vc1@172.16.0.163:5060>
supported: timer
Session-Expires: 180;refresher=uac
max-forwards: 70
Content-Type: application/sdp
Content-Length: ...

v=0
o= 0 0 IN IP4 172.16.0.163
s=
c=IN IP4 172.16.0.163
t=0 0
m=audio 4050 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=video 4060 RTP/AVP 98
a=rtpmap:98 MP4V-ES/90000
m=application 4070 RTP/AVP 99
a=rtpmap:99 MP4V-ES/90000
a=X-application: sharpVideoStreamShare }
```

103

To the extent it is argued that Toya's forwarding hops do not involve relay apparatuses, Tucker discloses transmitting video conference data through an intermediary server or relay apparatus. EX1003, ¶[102]. Tucker teaches a system comprising "a server configured to provide a website accessible by a remote user through a network connection" and a set-top box or "a television forwarding device in communication with the server." EX1005, claim 14, [0004], [0019], [0059], FIG1. Tucker's server mediates the video conference between the remote user's communications device and the television forwarding device or set-top box device, functioning as a relay for the conference signals. EX1005, ¶¶[0003]-[0005], [0019]-[0023], [0059] claims 14-16; EX1003, ¶[102]. The server, which may be communications management server 112 or 404, routes media content and video communications between one or more communications devices. EX1005, ¶¶[0019], [0065]; EX1003, ¶[102].

FIG. 1



In the combination, Toya's video communication device would transmit both the camera video data and the externally obtained content data through Tucker's intermediary server (relay apparatus) rather than directly to the counterpart device. EX1003, ¶[103]. A POSITA would have been motivated to route the data through a relay apparatus for the same reasons discussed in the motivation to combine—

centralized management, authentication, and security—and because relay-based architectures were the predominant model for enterprise video conferencing. EX1003, ¶[103]. This combination is the predictable use of a known technique (server-mediated data relay) to improve a similar device (Toya’s conferencing terminal) in the same way (routing video and content data through a centralized relay for management and security purposes). EX1003, ¶¶[103]-[104].

10. [3.a]/[10.a]

Tucker discloses this element, and the combination with Toya renders it obvious. Tucker teaches a system architecture in which a server mediates video conference sessions between remote users and television forwarding devices/set-top boxes. EX1005, ¶¶[0003]-[0005], [0019]-[0023], [0059]. claims 14-16. The communications management system 112 embodiment of Tucker’s server “may include any number of servers, routers, switches, or advanced intelligent devices.” EX1005, ¶[0019] Given that the communications management system 112 may include any number of servers, a POSITA would understand that it is necessary that one be selected. EX1003, ¶¶[105]-[106]. Similarly, Tucker discloses that “the communications management system 404 may buffer, process, or **route** the communications signals, packets, or data to facilitate the communications.” A POSITA would have understood that “routing” involves selecting intermediate stops through which data, such as packets, are relayed. EX1003, ¶[106].

Moreover, in enterprise video conferencing systems, it was well-known to deploy multiple relay servers across different geographic locations and to select the optimal relay based on network conditions such as latency, proximity, and available bandwidth. EX1003, ¶[107].

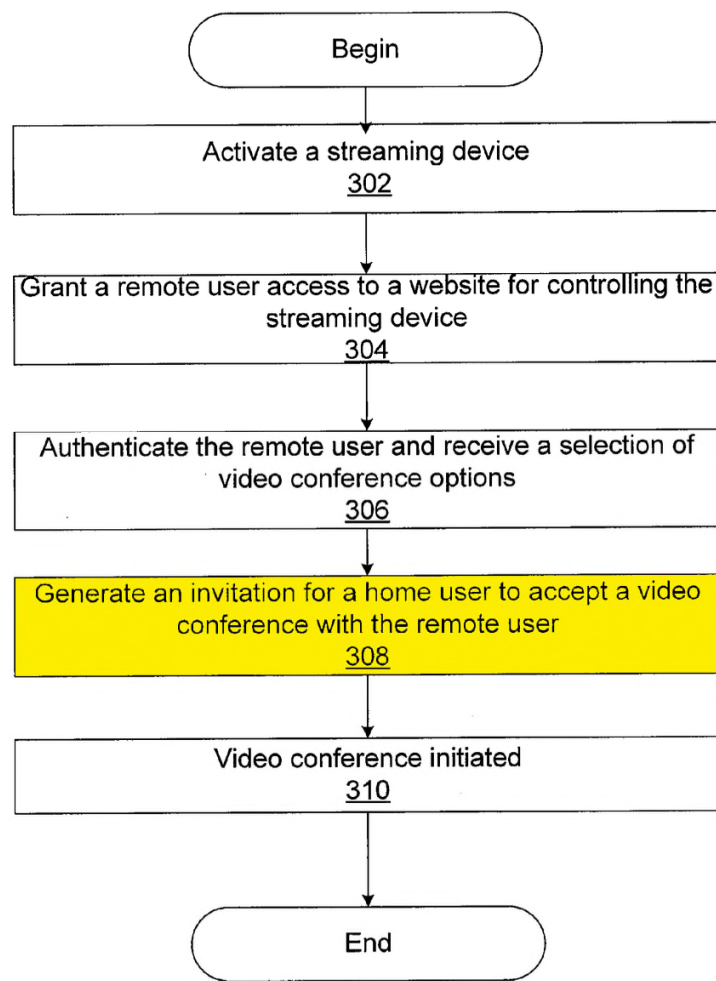
Additionally, Toya's IP/SIP-based forwarding mechanisms, which Toya acknowledges by including "max-forwards" in SIP headers, involves selecting between intermediate proxy servers or routing nodes for relaying data. EX1003, ¶[108]

A POSITA implementing Tucker's centralized server architecture with Toya's conferencing system would have found it obvious to select a relay apparatus from among multiple available relays based on network proximity and performance metrics. EX1003, ¶[109]. This was a known optimization in relay-based conferencing systems, and selecting among plural relays to minimize latency and maximize quality was standard practice well before the '917 Patent's priority date. EX1003, ¶[109]. The combination is the predictable use of known prior art elements (Tucker's server-mediated relay architecture; well-known relay selection techniques based on network metrics) according to known methods to yield predictable results (selecting the optimal relay apparatus for a video conference session from among multiple available relays). EX1003, ¶¶[109]-[110].

11. [3.b]/[10.b]

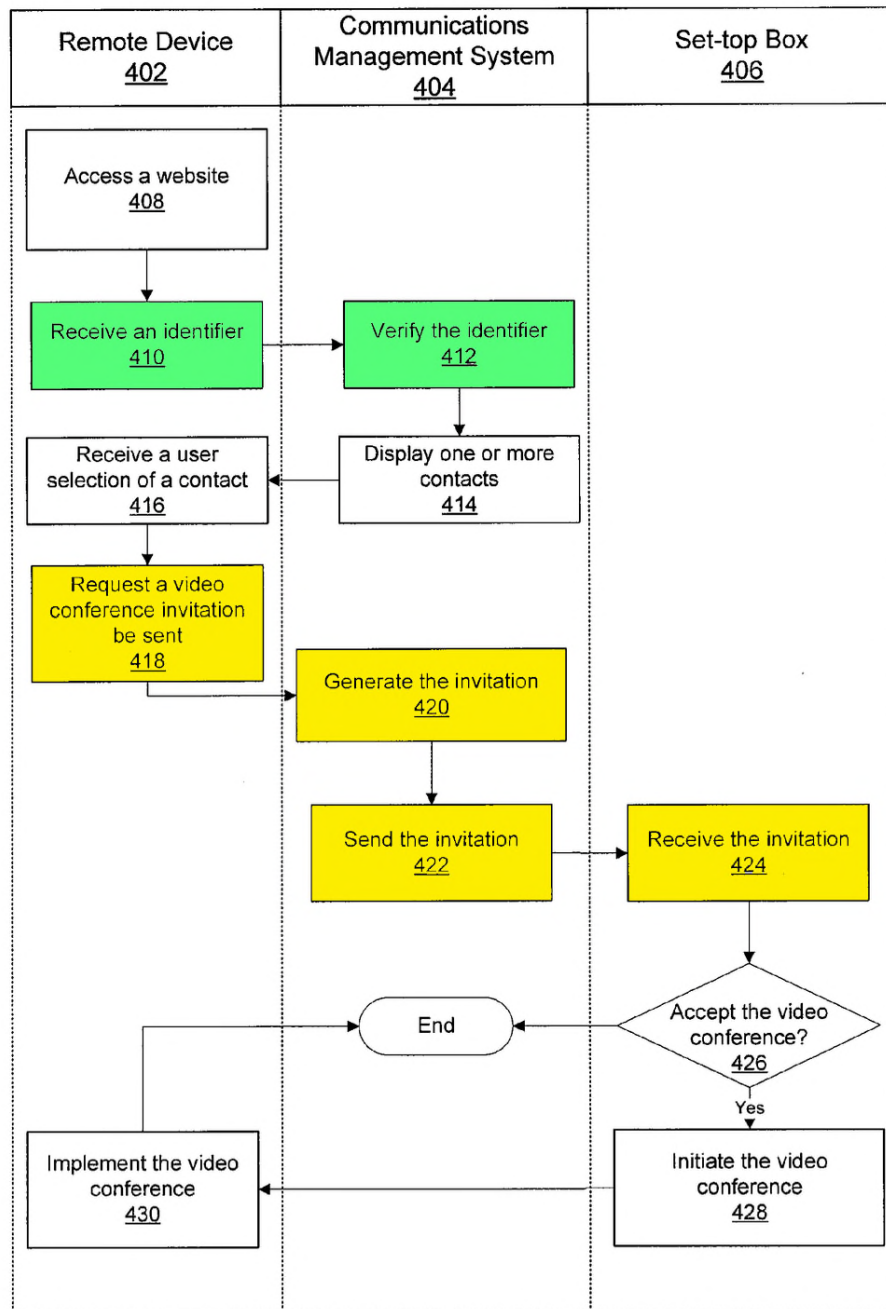
Tucker discloses this element. Tucker teaches that when a remote user selects to initiate a video conference with a local user, the system sends an invitation to the television forwarding device or set top box to notify the local user that a remote user has requested communication. EX1005, ¶¶[0003]-[0005],[0016],[0059],[0064]-[0065] claim 1, FIG3; EX1003, ¶[111]-[112].

FIG. 3



The server identifies which remote user has requested the start of communication and conveys that information to the television forwarding device or set-top box (the receiving terminal), enabling the local user to know who is requesting the conference and to accept or decline. EX1005, ¶¶[0003]-[0004]. [0022]-[0023], claims 1, 14, FIG4; EX1003, ¶[113].

FIG. 4



The invitation sent from the server to the television forwarding device or set-top box—which identifies the requesting remote user—constitutes “terminal identification information for identifying another transmission terminal that has

requested a start of communication.” EX1003, ¶114]. The server, for example communications management system 112 or 404, which manages multiple authorized users in its database, constitutes the “management system” that provides this information “from among a plurality of transmission terminals.” EX1003, ¶114].

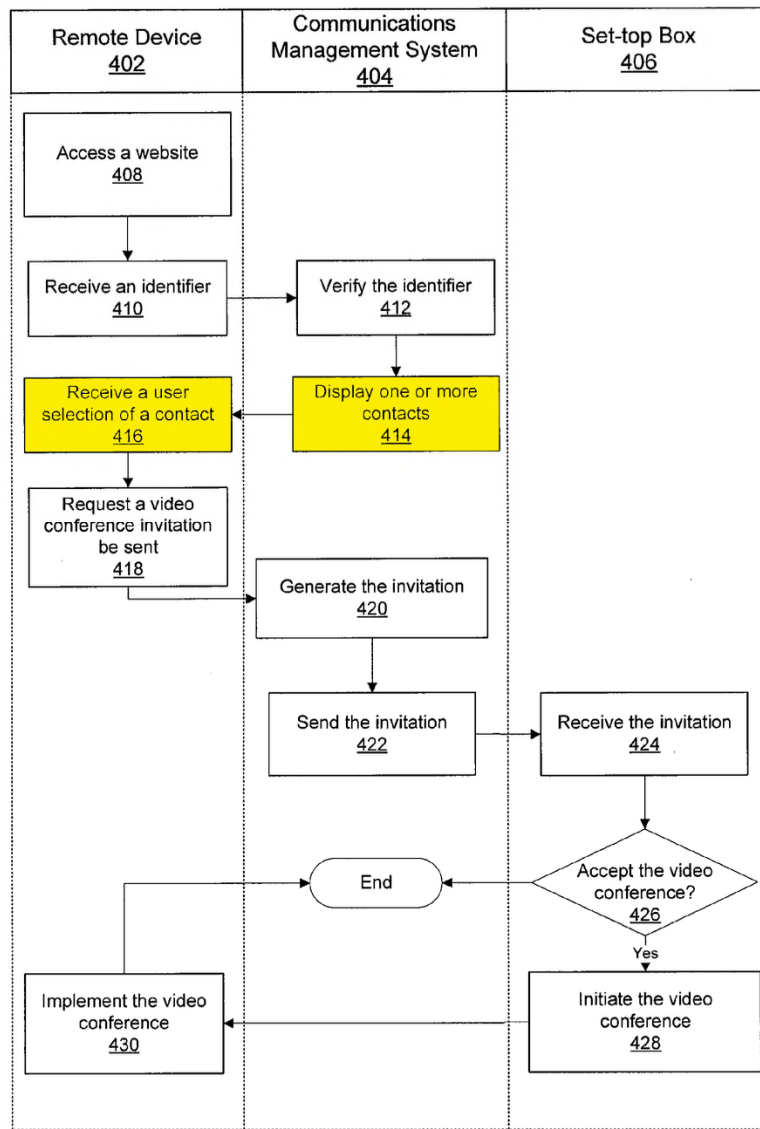
In the combination, Tucker’s management server—which maintains a database of multiple authorized terminals and mediates session initiation by sending invitations identifying the requesting user—provides terminal identification information to the receiving terminal, enabling it to identify which of the plurality of managed terminals has requested a start of communication. EX1003, ¶115]. A POSITA would have understood that informing a receiving terminal of the identity of a requesting terminal was a fundamental and known feature of any managed, multi-terminal video conferencing system. EX1003, ¶115]. This is further confirmed by the fact that Tucker’s system already performs this function when it sends an invitation identifying the remote user to the television forwarding device. EX1003, ¶115]. The combination thus satisfies this limitation. EX1003, ¶¶115]-[116].

12. [7.a]/[14.a]

Tucker discloses this element. Tucker teaches that the server provides the user with a list of available contacts for video conferencing. EX1005, ¶[0003]-

[0004], [0022]-[0023], [0061], claim 1. Specifically, Tucker discloses that “the selection of the user is made using a network address book that lists a plurality of contacts, wherein the plurality of contacts are received based on user input through the set-top box.” EX1005, claim 3, [0023], [0054], [0062]. The server maintains a database of authorized users and provides the requesting user with information about which contacts are available for communication. EX1005, claims 3, 14-15, [0023], [0054], [0061]-[0062]. The network address book listing a plurality of contacts constitutes “information of destination candidates associated with the first transmission terminal,” and the server that stores and provides this information constitutes the “management system.” EX1003, ¶¶[117]-[118]. For example, communications management system 404 displays a list of contacts from which the user of the remote device can select. EX1005, FIG4; EX1003, ¶ [118].

FIG. 4



In the combination, after Toya's video communication device authenticates with Tucker's management server, the server provides a list of destination candidates—i.e., other authenticated terminals available for communication—to the first terminal. EX1003, ¶[119]. A POSITA would have understood that receiving a

list of available conferencing destinations from a centralized server was a predictable feature of managed video conferencing systems. EX1003, ¶¶[119]-[120].

13. [7.b]/[14.b]

Tucker discloses this element. Tucker teaches that after the contacts are presented to the user, the system “receiv[es] a selection of a user for the remote user to communicate with through the video conference.” EX1005, ¶[0003]-[0004], [0054], [0063]-[0065], claim 1. As illustrated in Tucker’s FIG6, the user interface presents a “Select Participant(s)” step in which the user chooses from among available contacts such as “Home,” “Mom and dad,” and “Guest House.” EX1005, FIG6, ¶¶[0071]-[0074]. The user’s selection of a desired contact from among the listed destination candidates constitutes “receiv[ing] a selection from among the received information of the destination candidates.” EX1003, ¶¶ [121]-[122].

In the combination, after Tucker’s management server provides the list of destination candidates to Toya’s video communication device, the user selects one of those candidates through the device’s user interface. EX1003, ¶[123]. A POSITA would have understood that presenting a list of available destinations and receiving a user selection was a standard step in initiating a managed video conference session. EX1003, ¶¶ [123]-[124].

14. [7.c]/[14.c]

The combination of Toya and Tucker teaches this element. Tucker teaches that, in response to the user's selection, the system establishes the video conference with the selected contact. Specifically, Tucker discloses sending an invitation to the television forwarding device or set-top box, and implementing the video conference between the remote user and the user in response to the user accepting the invitation. EX1005, ¶[0003], [0046], claim 1. The video conference session is thus established with the specific terminal corresponding to the user's selection from among the destination candidates. EX1003, ¶¶[125]-[126].

Toya provides the underlying session-establishment mechanism. EX1004, 16:51-17:10, FIG9. Toya discloses that after the user selects a counterpart device, the communication control section 2 establishes “a call session with another video communication device serving as a counterpart device” using SIP signaling. EX1004, 16:58-17:6. In the combination, after Toya's video communication device receives the list of destination candidates from Tucker's management server and the user selects one of those candidates, Toya's SIP-based session establishment mechanism initiates a call session with the selected counterpart device—the “second transmission terminal corresponding to information of the thus selected destination candidate.” EX1003, ¶[127]. A POSITA would have understood that establishing a conferencing session with a user-selected destination was the natural and predictable

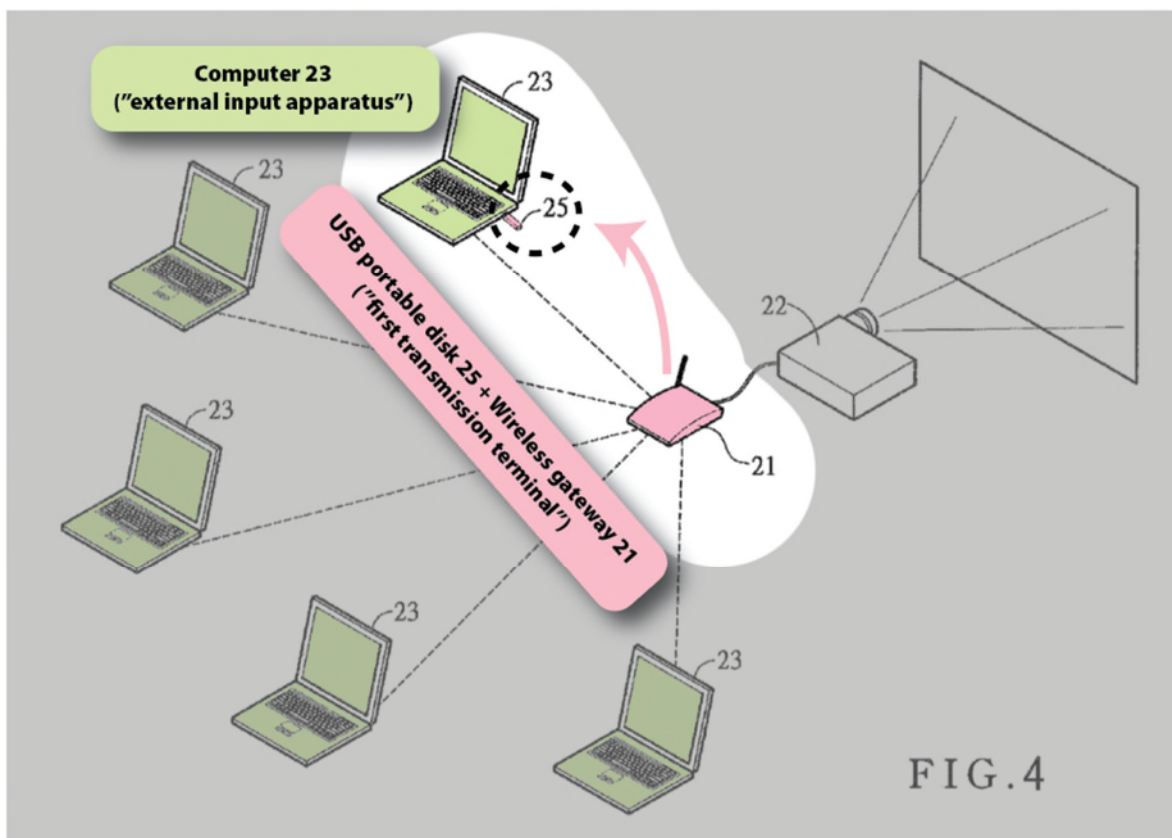
outcome of combining Toya's SIP-based session establishment with Tucker's server-mediated participant selection. EX1003, ¶¶ [127]-[128].

B. Ground 2: Toya in view of Tucker and Further in View of Chang Renders Obvious Claims 4-6, 11-13

The permission-request, program-transmission, and conditional-installation steps of claims 4–6 and 11-13 are nothing more than the routine application of well-known software deployment techniques that a POSITA would have found obvious when implementing Toya's content-sharing architecture. EX1003, ¶[129].

However, to the extent a POSITA wanted additional details beyond Toya in view of Tucker about the permission-request, program-transmission, and conditional-installation mechanisms recited in claims 4–6 and 11-13 Chang discloses these elements. Chang discloses a plug-and-show USB portable disk that, when connected to a presenter's laptop during a conference, automatically delivers screen-capture software ("green software") from the conferencing hub system to the laptop, causes the software to execute on the laptop to capture presentation frame data, and forwards the captured data through the laptop to the wireless gateway for display to conference participants—all without requiring pre-installation on the laptop. EX1007, Abstract, 4:55-5:21, FIGS. 2, 4; EX1003, ¶¶[130]-[131]. In this architecture, the wireless gateway and its associated USB portable disk constitute the conferencing hub (analogous to the "first transmission terminal" that is logged

into the conference), and the presenter's laptop constitutes the "external input apparatus" that has not logged into the conferencing management system. EX1003, ¶[131]. A POSITA would have understood that the USB disk is functionally a component of the hub—it is the physical mechanism by which the hub delivers its screen-sharing program to external participant laptops, just as the '917 Patent's transmission terminal stores and transmits its display data acquiring unit to the external input apparatus. EX1003, ¶[131].



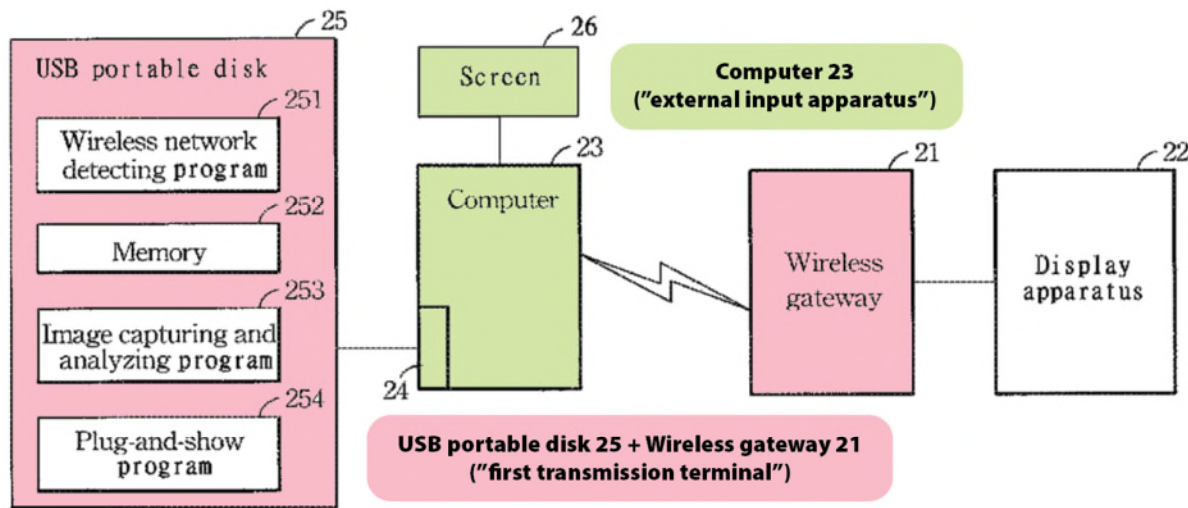


Fig. 2

As explained below, Chang's disclosures map directly to each limitation of claims 4–6. For claim 4, Chang teaches that when the USB portable disk engages with the laptop's USB port, the auto-run plug-and-show program triggers a request for the laptop to permit execution of the image capturing and analyzing program (claim 4.a), and upon permission the program executes on the laptop to capture display data that is forwarded to the wireless gateway (claim 4.b). EX1003, ¶[132]. For claim 5, Chang teaches that the conferencing hub system transmits the screen-capture program to the laptop via the USB portable disk upon connection. EX1003, ¶[132]. For claim 6, Chang's green-software architecture satisfies the conditional-installation requirement: because the program is never permanently installed on the

laptop—it is loaded fresh upon each connection and removed upon disconnection—the system necessarily transmits the program each time the connection is made, precisely because the program is not installed on the external device when the connection occurs. EX1007, 5:1-7; EX1003, ¶[132].

A POSITA would have been motivated to combine Chang with Toya and Tucker because all three references are in the same field of conferencing content-sharing systems, because Chang directly solves the problem of enabling seamless screen sharing from external devices without pre-installation (the same problem the '917 Patent purports to address), and because the combination yields the predictable result of a video conferencing terminal that automatically provides a screen-capture program to a connected external laptop so that the laptop's display data can be shared with remote conference participants over the established session. EX1003, ¶¶[133]-[138]; *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007).

1. Motivation to Combine

Same Field of Endeavor: Chang, Toya, and Tucker are all directed to systems for sharing presentation content or video data during conferences or meetings. Chang specifically addresses wireless presentation systems in which “plural representatives with their own computers may present to show their presentation files pre-stored in their own computers” during a “presentation

conference.” EX1007, 1:43-54. This is the same conference content-sharing scenario addressed by Toya and the ’917 Patent. EX1003, ¶[134]. A POSITA designing a video conferencing terminal with content-sharing capabilities from external devices would have naturally looked to Chang’s plug-and-show architecture. EX1003, ¶[134].

Chang Solves a Problem That Toya and Tucker Do Not Address: The Toya/Tucker combination provides the foundational video conferencing and content-sharing architecture but does not focus on how the external device transmits image or video data to the terminal. For example, Toya is silent on how a mobile phone would transmit the image/video if it does not have software installed for performing such transmission, or how such software might be seamlessly and conveniently installed. Chang provides disclosure on how such functionality would be implemented. Chang identifies the need—“a specific drive program for the wireless projector is needed to be installed into the computer prepared for a corresponding wireless projector”—and provides the solution: a plug-and-show USB disk that automatically provides and executes green software on the external computer upon connection, without requiring pre-installation. EX1007, 1:32-2:56, Abstract. A POSITA would have been motivated to incorporate Chang’s plug-and-show program-delivery mechanism into the Toya/Tucker combination to enable sharing of screens, videos, or images from any external device without requiring the

external device to already have any necessary content-sharing software installed. EX1003, ¶[135].

Chang’s Express Motivation: Chang expressly identifies the motivation for its approach: eliminating the need for pre-installation of drive programs on each presenter’s computer, avoiding “time needed for the installation as well as the restart process” that “may ruin his/her presentation or at least cost the conference flow,” and enabling presentation “any time after the plug-and-show USB portable disk is plugged into the computer.” EX1007, 1:57-2:16, 3:51-65. These same motivations apply directly to Toya’s content-sharing system: a video conferencing terminal that can automatically provide necessary software to any connected external laptop—without requiring pre-installation—delivers the same plug-and-show convenience in the video conferencing context. EX1003, ¶[136].

Predictable Combination of Known Elements: The combination of Toya, Tucker, and Chang is the predictable use of known prior art elements according to known methods to yield predictable results. *KSR*, 550 U.S. at 415-421. Toya teaches a video conferencing terminal that receives content from external devices and forwards it over an established session. EX1004, 17:58-18:49, 19:28-50, 20:23-32. Tucker teaches centralized authentication for session establishment. EX1005, [0003]-[0005], [0022]-[0023] claims 1, 13-15. Chang teaches delivering an image transfer program from a conferencing hub (via USB disk) to an external computer

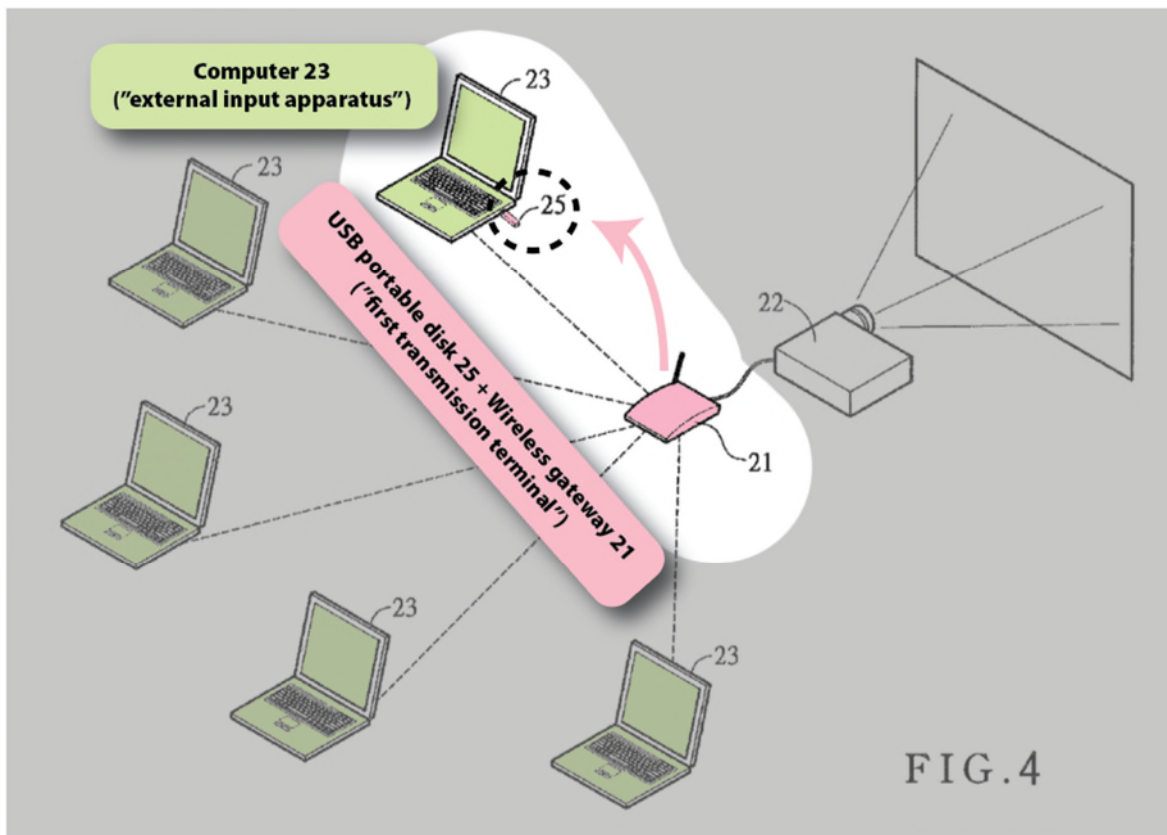
upon connection, with the program automatically executing to capture and forward display data to the conferencing system—all without pre-installation. EX1007, Abstract, 4:55-5:21. Incorporating Chang’s plug-and-show program-delivery mechanism into the Toya/Tucker combination yields the entirely predictable result: when an external laptop connects to the video conferencing terminal, the terminal provides a screen-capture program to the laptop, the laptop requests permission to execute the program, the program captures the laptop’s display data, and the captured image data is forwarded to the conferencing counterpart over the established session. EX1003, ¶[137].

Reasonable Expectation of Success. A POSITA would have had a reasonable expectation of success because Chang’s plug-and-show architecture operates at the same physical interface (USB connection between an external computer and a conferencing hub) as the ’917 Patent’s external input apparatus connection. EX1003, ¶[138]. The modification requires no changes to Toya’s video conferencing session architecture or Tucker’s authentication mechanism—it merely adds Chang’s program-delivery and auto-execution mechanism at the point where the external device physically connects to the terminal. EX1003, ¶[138].

2. [4.a]/[11.a]

Chang discloses this element. In Chang’s system, the USB portable disk 25 stores a plug-and-show program 254 that is an auto-run program. EX1007, 5:1-

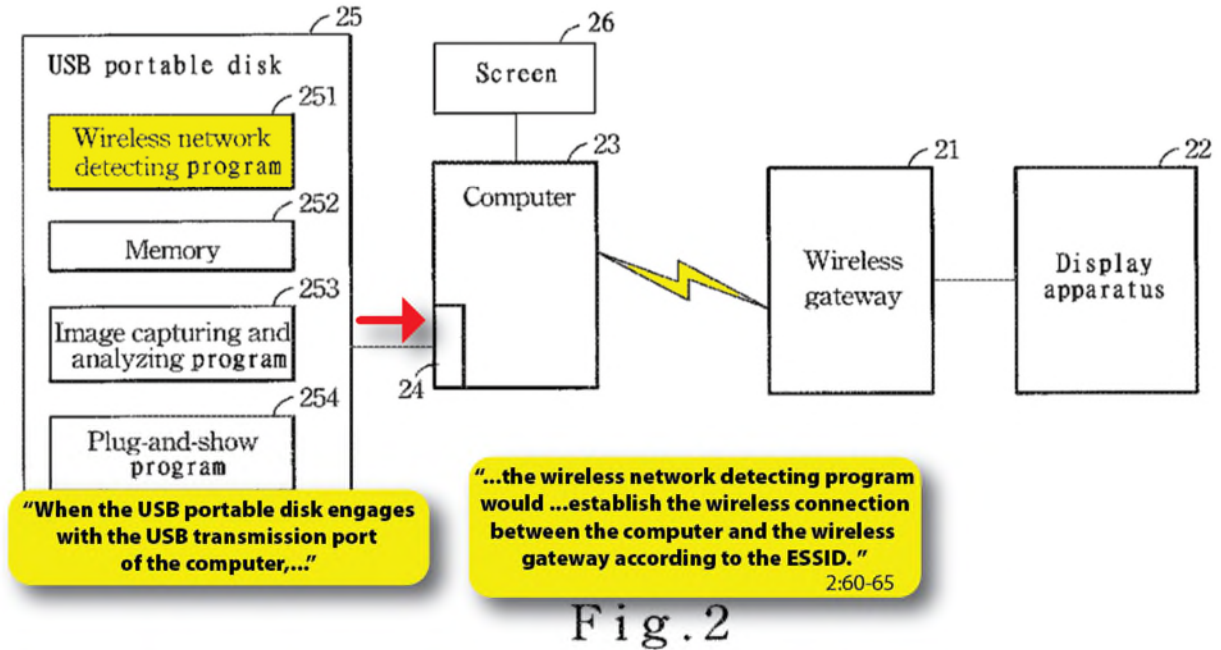
7. When the USB portable disk 25 engages with the USB transmission port 24 of the computer 23, “the computer 23 will automatically execute any instruction from the plug-and-show program 254.” EX1007, 5:1-7. In Chang, the wireless gateway 21 (together with the USB portable disk 25, which is part of or associated with the gateway/hub system) is the “first transmission terminal,” and the computer 23 (the presenter’s laptop) is the “external input apparatus.” EX1003, ¶¶[139]-[140]. The USB portable disk 25 is the physical mechanism by which the first transmission terminal provides its program to the external input apparatus—it is functionally part of the conferencing hub infrastructure, as a POSITA would have understood that the dongle/USB disk is the hub’s accessory for enabling screen sharing from external laptops. EX1003, ¶[140].



When the computer 23 detects the engagement of the USB portable disk, the auto-run function triggers the plug-and-show program, which constitutes a request—initiated by the USB disk (associated with the terminal/hub)—for the computer to permit execution of the image capturing and analyzing program 253. EX1007, 5:1-8. Under USB auto-run protocols, the host computer's operating system receives the auto-run request and determines whether to permit execution—Windows auto-run prompts, for example, ask the user to confirm execution of software from removable media. A POSITA would have understood that this auto-run engagement

constitutes a “request for permission to execute a program that is for obtaining data in the external input apparatus.” EX1003, ¶[141].

Moreover, Chang’s USB portable disk 25 stores the plug-and-show program 254, the image capturing and analyzing program 253, and the wireless network detecting program 251. EX1007, 4:49-5:21. When the USB is inserted into the computer (the claimed external input apparatus), the wireless network detecting program is launched, to establish a connection to Chang’s wireless gateway (the claimed transmission terminal). EX1007, 2:58-65. A POSITA would have understood that if the computer is not permitted by the wireless network to connect, the other programs, which capture and then transmit images wirelessly to the wireless gateway, should not be executed, as such transmission would be impossible. EX1003, ¶[142].



Toya provides motivation for this sort of permission-based system, noting the importance of preventing content from unexpected sources from being transmitted over the network. EX1004, 5:14-28; EX1003, ¶[143].

A POSITA would have found it obvious to implement a permission-request mechanism in which the external input apparatus asks the conferencing terminal for authorization before executing a data-capture program. EX1003, ¶[144]. This pattern ensures that (1) the terminal user retains control over what data is captured and shared during the conference—a straightforward security and usability consideration that was well-known in the design of connected-device architectures, and (2) image capture and transmission software does not execute when such

transmission is impossible, which would waste computing resources. EX1003, ¶¶[144]-[145].

3. [4.b]/[11.b]

Chang discloses this element. Upon the computer 23 permitting execution, the plug-and-show program 254 causes the computer 23 to execute the image capturing and analyzing program 253, which captures and analyzes the presentation frame data transmitted from the computer to the screen and generates and forwards an analysis result of the presentation frame data to the wireless gateway through the computer. EX1007, 2:66-3:3, 5:10-21. The image capturing and analyzing program 253 executes *on the computer 23* (the external input apparatus) and captures presentation frame data (the “second video data”) from the computer’s display output. EX1007, 2:66-3:17. The captured data is then forwarded from the computer 23 to the wireless gateway 21 (and ultimately to the display apparatus 22 for the conference). EX1007, 2:66-3:17, 4:39-5:8; EX1003, ¶¶[146]-[147].

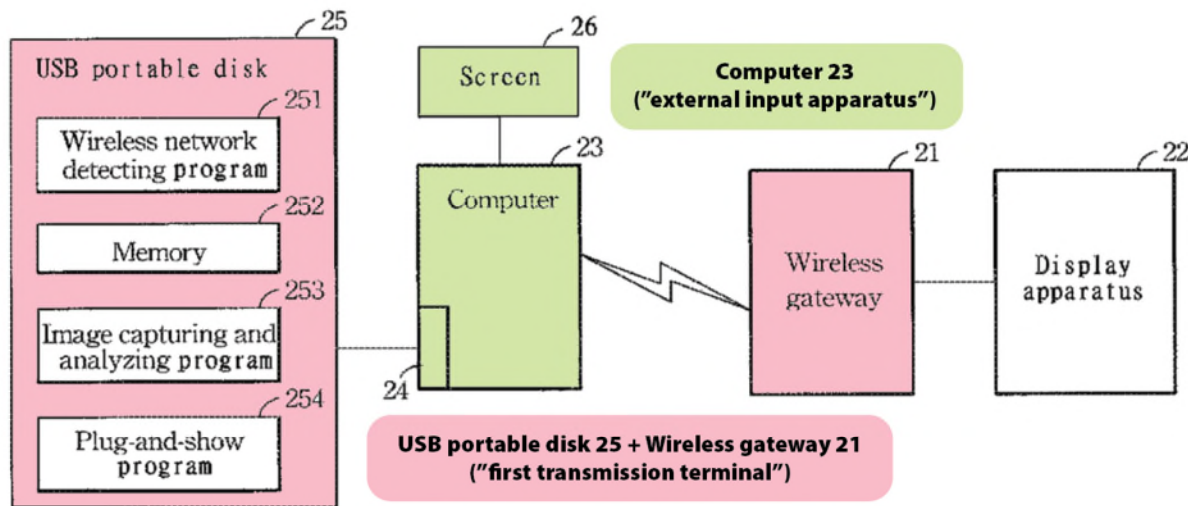


Fig. 2

In the combination with Toya and Tucker, the wireless gateway 21 (the first transmission terminal, which is logged into the conferencing system) receives the captured display data from the computer 23 (the external input apparatus that has not logged into the management system) and forwards it to the remote conference participants. EX1003, ¶[148]. This maps precisely to claim 4.b: in response to permission, the program executes in the external input apparatus to obtain data, and the processing circuitry of the first terminal receives the obtained data from the external apparatus. EX1003, ¶[148].

A POSITA would have understood that conditioning the execution of a data-acquisition program on receiving permission from the host terminal was a routine and predictable design choice. EX1003, ¶[149]. This pattern provides the terminal

user with an opportunity to authorize or decline the data capture before it occurs, which was a well-known approach to managing device interactions in conferencing and collaboration systems. EX1003, ¶¶[149]-[150].

4. Claim 5/12

Chang discloses this element. Chang's USB portable disk 25 stores the plug-and-show program 254, the image capturing and analyzing program 253, and the wireless network detecting program 251. EX1007, 4:49-5:21. When the USB portable disk 25 is inserted into the computer 23's USB transmission port 24, these programs are provided from the USB disk to the computer for execution. EX1007, 5:1-8. The USB portable disk 25, as an accessory of the wireless gateway/conferencing hub system, constitutes the mechanism by which the first transmission terminal transmits its programs to the external input apparatus. EX1003, ¶¶[151]-[152].

A POSITA would have understood that the USB portable disk is functionally equivalent to a component of the conferencing hub—it is the physical carrier that the hub system uses to deliver its screen-capture software to the external laptop. EX1003, ¶[153]. Commercial wireless presentation systems such as those manufactured by Awind (the assignee of Chang), Barco (ClickShare), and Crestron have long used USB dongles as the mechanism by which the conferencing hub transmits its screen-sharing program to participant laptops. EX1003, ¶[153]. A

POSITA would have recognized that whether the program is stored on a USB dongle physically associated with the hub or in internal storage of the terminal itself, the result is the same: the first terminal transmits a program to the external device. EX1003, ¶[153].

Moreover, transmitting a program from a host device to a connected peripheral for execution on the peripheral was a well-known software deployment technique, and a POSITA would have found it obvious to transmit a data-acquisition program from Toya's video communication device to the connected external device in order to enable content capture and sharing. EX1003, ¶¶[154]-[155].

5. Claim 6/13

Chang discloses this element. Chang's programs are "green software"—software "that can be executed directly in the computer without any pre-installation." EX1007, 4:55-67. Chang explains that "[t]he green software can be stored in the USB portable disk 25, and thus can be run immediately as soon as the USB portable disk 25 is engaged with the USB transmission port 24 of the computer 23. While the USB portable disk 25 disengages with the computer 23, the green software can be removed from the computer 23 automatically." EX1007, 4:56-62. EX1003, ¶¶[156]-[157].

This green-software architecture discloses the conditional-installation logic of claim 6: because the program is never permanently installed on the external

computer—it is loaded fresh each time the USB disk is connected and removed when disconnected—the system necessarily provides the program to the computer each time the connection is made, precisely because the program is *not installed* on the computer when the connection occurs. EX1003, ¶[158]. Chang expressly identifies this as an advantage over the prior art, which “need[ed] to install a proper drive program immediately at the conference site” and which “different manufacturers provide different drive programs for their products.” EX1007, 1:55-2:16. Chang’s solution—transmitting the program from the USB disk (associated with the hub) to the computer only upon connection, because it is never permanently installed—discloses the conditional-installation requirement of claim 6. EX1003, ¶[158].

Moreover, a POSITA would have understood that implementing an explicit check before transmitting the program is a trivial and predictable optimization of Chang’s approach: if the green software happens to already be present on the computer (e.g., from a prior connection that was not properly cleaned up), there is no need to re-transmit it. Adding such a check to Chang’s system would have been a routine software engineering step. EX1003, ¶[159].

Moreover, this claimed conditional-installation pattern—checking whether software is already present before transmitting it—was a well-known technique in software deployment, and a POSITA implementing a content-sharing system would have found it obvious to check for the presence of the required program on the

external device before transmitting it, in order to avoid redundant installations and reduce network overhead. EX1003, ¶¶ [160]-[161].

C. Ground 3: Toya in view of RFC 3261 Renders Obvious Claims 1-3, 8-10, 15

Toya in view of RFC 3261 renders obvious every limitation of claims 1-3, 8-10, 15. Toya provides the foundational video conferencing architecture in which a communication device establishes a call session with a counterpart device, captures and transmits video data, receives content data from an external source, and forwards that content to the counterpart over the established session. EX1003, ¶[162]. Toya discloses that this can be accomplished using Session Initiation Protocol (SIP). EX1004, 16:65-17:6. Toya does not, however, explicitly disclose that the terminals log into a centralized management system by transmitting a login request before establishing the communication session. EX1003, ¶[162]. RFC 3261 discloses a server-mediated video conferencing system in which terminals must log into a managing registrar system prior to videoconferencing. EX1006, §22, §26.1.1; EX1003, ¶[162]. All other limitations of claims 1-3, 8-10, 15 are disclosed by Toya as explained above in Ground 1.

1. RFC 3261

RFC 3261 was published by the Internet Engineering Task Force (IETF) in June 2002, approximately eight years before the '917 Patent's earliest priority date

of May 6, 2010, and qualifies as prior art at least under 35 U.S.C. § 102(b) (pre-AIA). EX1003, ¶[163].

The document lists June 2002 as its publication date, and provides that “Distribution of this memo is unlimited.” EX1006, p.1. The IETF Datatracker—the official publication index maintained by the Internet Engineering Task Force—lists RFC 3261 with a date of June 2002. EX1006. The document header on each page of the RFC itself bears the legend “RFC 3261 SIP: Session Initiation Protocol June 2002,” which serves as an internal publication-date indicator analogous to a copyright notice. EX1006, p.2 (header). The document also provides a “Copyright Notice” reciting “Copyright (C) The Internet Society (2002).” EX1006, p.1. The NISP Nation standards registry independently catalogs RFC 3261 with a publication date code of “2002-06”. EX1017. Additionally, Petitioner’s expert was a co-author for RFCs 3170, 3171, and 3611 published in September 2001, August 2001, and November 2003, respectively. EX1003, ¶[164]. Together, these corroborating sources leave no ambiguity regarding the date on which RFC 3261 became a publicly available printed publication for purposes of § 102(b).

Additionally, subsequent IETF documents that update or reference RFC 3261 uniformly cite it with a June 2002 date. For instance, the bibliographic entry in draft-ietf-sipcore-priority (later published as RFC 6878) states: “Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M.,

and E. Schooler, ‘SIP: Session Initiation Protocol’, RFC 3261, June 2002.” EX1018, at Section 4.1. Petitioner’s expert cited to RFC 3261 in a work published in 2006. EX1019, 15. EX1003, ¶[165]. This consistent bibliographic practice across the IETF corpus is itself evidence that the document was publicly accessible as of that date, because the citing authors necessarily had access to RFC 3261 in order to reference it.

RFC 3261 is also discussed in U.S. Pat. Publ. No. 2004/0062204A1 (EX1020), based on an application filed Sep. 30, 2002, where it is described as being published at <http://www.ietf.org/rfc/rfc3261.txt> in June 2002. EX1003, ¶[166].

Petitioner’s expert attended SIP working group meetings, along with other audio/video related working groups, in the years prior to the standardization of SIP as RFC 3261. EX1003, ¶[167]. He also personally accessed RFC 3261 from publicly available sources shortly after its June 2002 publication and on numerous occasions thereafter. EX1003, ¶¶[167]-[168]. The RFC Editor has maintained RFC 3261 on its publicly accessible website (<https://www.rfc-editor.org>) and at the IETF’s own web repository (<https://www.ietf.org/rfc/rfc3261.txt>) since the document’s initial publication. EX1006; EX1003, ¶[168] Petitioner’s expert, while in the United States, downloaded RFC 3261 multiple times from the RFC Editor website and the IETF website, both of which are freely accessible to any member of the public without any subscription, paywall, or access restriction. EX1003, ¶[168]. The IETF’s

longstanding open-access policy ensures that all published RFCs are available to the global public at no cost. Petitioner's expert further confirms personal knowledge that RFC 3261 was extensively discussed, distributed, and relied upon within the networking and telecommunications community beginning in 2002, including at IETF working group meetings and industry conferences. EX1003, ¶[168]. Accordingly, there is no genuine dispute that RFC 3261 was publicly accessible years before the May 6, 2010 earliest priority date of the '917 Patent.

2. Motivation to Combine

A POSITA would have been motivated to incorporate RFC 3261's authentication mechanisms into Toya's SIP-based video conferencing and content-sharing system for several independently sufficient reasons. EX1003, ¶[169].

Toya's Express Concern with Security and Use of SIP: Toya expressly discloses that it is desirable to decrease the possibility that an unexpected communication device can access the content data. EX1004, 21:10-20. Toya further discloses that the use of SIP protocols for communications. EX1004, 27:52-28:2; EX1003, ¶[170].

Given Toya's extensive disclosures involving using SIP and its express disclosure of the desirability of ensuring that only authorized devices can access content data, a POSITA would have been motivated to combine Toya with SIP for

authentication as disclosed in RFC 3261, which defines the Session Initiation Protocol standard. EX1003, ¶[171].

Same Field of Endeavor: Toya and RFC 3261 are in the same field of endeavor: both are directed to conferencing systems that establish sessions between remote participants and transmit multimedia data over a communication network. Toya discloses a “video communication device” that “function[s] as a television conference system terminal device” and establishes “a call session with another video communication device serving as a counterpart device, thereby realizing reception and transmission of video data and audio data therebetween.” EX1004, 16:51-64. RFC 3261 likewise discloses a standard for “creating, modifying and terminating sessions with one or more participants,” including “multimedia conferences.” EX1006, Abstract, p. 1. Both references address how to manage the initiation and conduct of conferences between networked endpoints. EX1003, ¶[172]. A POSITA designing a video conferencing system with content-sharing capabilities would have naturally looked to both references. EX1003, ¶[172].

RFC 3261 Solves a Problem That Toya’s System Faces: Toya’s system faces a fundamental security and access-control problem that Toya does not focus on: how to ensure that only authorized users can initiate or participate in video conference sessions. EX1003, ¶[173]. Toya discloses that its video communication device establishes call sessions using SIP signaling, but Toya does not focus on

mechanisms for verifying the identity or authorization of the terminals before permitting the session to proceed. EX1004, 16:51-17:10. Without an authentication mechanism, any device with network access could potentially initiate a call session with Toya's video communication device, raising obvious concerns about unauthorized access and misuse. EX1003, ¶[173].

RFC 3261 directly solves this problem. RFC 3261 discloses a "registrar" which is a server that handles registration of authenticated entities which may participate in videoconferences. EX1003, ¶[174]. The registrar is a server that handles "REGISTER" requests, which associate a user with a particular terminal. EX1006, §6, 10.2. RFC 3261 also notes the threat of "registration hijacking," and suggests that a service "control access to its resources by authenticating requests that it receives" because devices "have an interest in ascertaining the identities of originators of requests." EX1006, §26.1.1. As RFC 3261 states, there is "the need for security services that enable SIP entities to authenticate the originators of requests." EX1006 § 26.1.1; EX1003, ¶[174].

RFC 3261 states that a registrar "SHOULD authenticate the UAC." EX1006, §10.3. RFC 3261 discloses a challenge-based mechanism for authentication that resolves the issue, identified in Toya, that an unauthorized party might otherwise access content data. EX1006, §22. Specifically, RFC 3261 discloses a login framework where, in response to an initial request from a client, the responding

server may issue a challenge, requiring the user's terminal to provide information proving identity. *Id.*; EX1003, ¶[175].

Predictable Combination of Known Elements: The combination of Toya and RFC 3261 is the predictable use of known prior art elements according to known methods to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007). Toya teaches a video conferencing terminal that establishes SIP-based call sessions, transmits camera video to a counterpart device, receives content data from external sources, and forwards that content to the counterpart over the established session. EX1003, ¶[176]. Toya further discloses specific details of the use of SIP protocols, such as the "INVITE" message. EX1004, FIGS. 10, 13. RFC 3261 discloses the specifications for the SIP protocol, including the INVITE message as well as authentication procedures and the use of registrars to manage conference participant registration. EX1003, ¶[176]. Incorporating registrars and authentication into Toya is merely the inclusion of additional SIP features, not addressed by Toya, into Toya's existing scheme. EX1003, ¶[176]. The authentication and registrar features disclosed by RFC 3261 are designed to work in conjunction with the INVITE and other SIP protocol features relied upon and disclosed by Toya. EX1003, ¶[176].

3. [1.b]/[8.b]/[15.b]

Toya does not explicitly disclose logging into a management system by transmitting a login request. RFC 3261 discloses this element.

RFC 3261 discloses a video conferencing system in which a user registers with a registration server, which is a management apparatus, before participating in conferences. EX1006, Abstract; §24.1. RFC 3261 teaches a “registrar” which is a server that handles registration of users who may participate in videoconferences, and, more specifically handles users’ “REGISTER” requests. EX1006, §10.3. RFC 3261 also explains that “authentication [is] usually required for registration” (EX1006, §24.1) because there is “the need for security services that enable SIP entities to authenticate the originators of requests.” EX1006, § 26.1.1; EX1003, ¶¶[177]-[178].

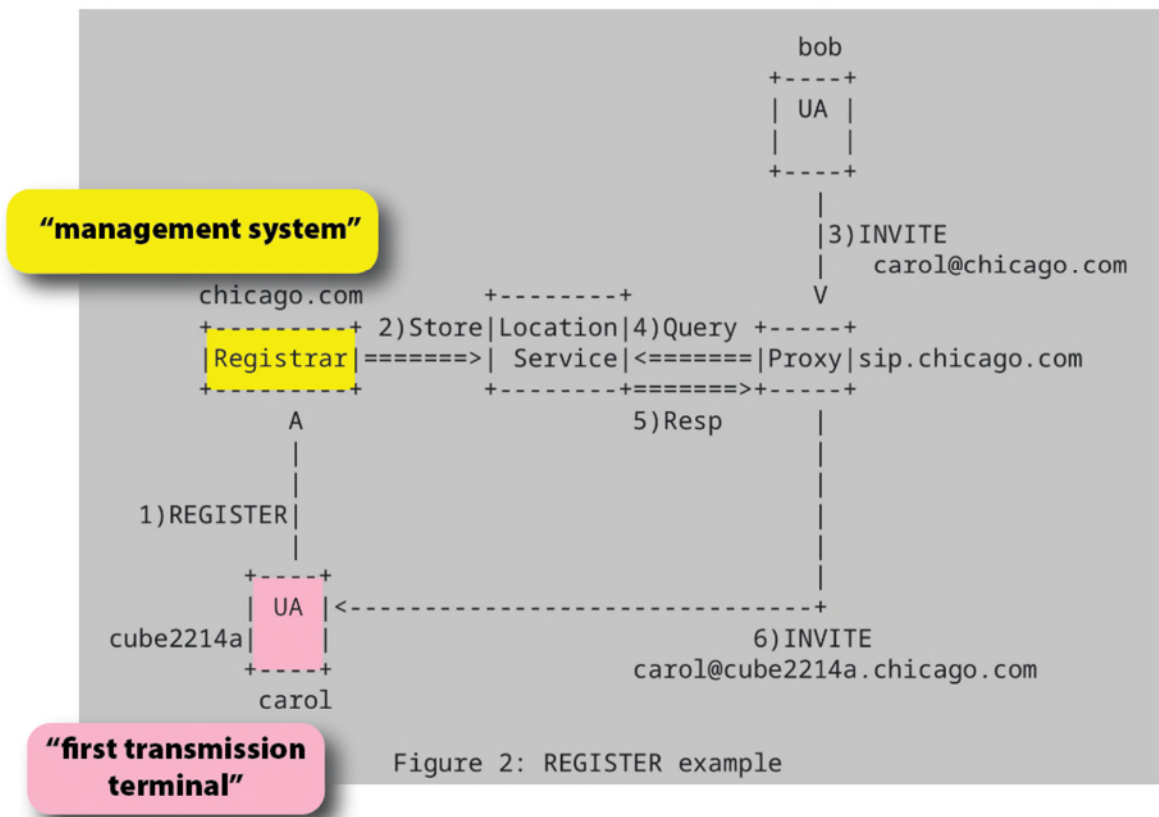


Figure 2: REGISTER example

RFC 3261 teaches that the user at a “UA” (first transmission terminal) submits a login request by providing “credentials” in response to an authentication challenge. EX1006, §26.2.3. The challenge, for example, may be part of a “401 response” to an initial registration request. EX1006, §§8.1.3.5, 21.4.2, 22.1-22.3. In response to the challenge, the challenged device must provide appropriate credentials to the registrar. EX1006, §22.1. By sending a REGISTER message with the authorization request header, the client is transmitting a login request to the registration server. EX1003, ¶¶[179]-[180].

D. Ground 4: Toya in view of RFC 3261 and Further in View of Chang Renders Obvious Claims 4-6, 11-13

For the same reasons as explained above in Ground 2, to the extent a POSITA wanted additional details beyond Toya in view of RFC 3261 about the permission-request, program-transmission, and conditional-installation mechanisms as recited in claims 4–6, 11-13, Chang discloses it. Toya’s video communication device 1 establishes call sessions with counterpart devices using SIP signaling as defined in RFC 3261, transmits camera video data over the established session, receives content data from external devices through local interfaces (Bluetooth, infrared, SD card, Ethernet), and forwards that content to the counterpart device for shared viewing during the video conference. EX1003, ¶[181]. RFC 3261 supplies the detailed SIP-based session establishment protocol—including INVITE, authentication, and session management—that underpins Toya’s conferencing architecture, rendering obvious the management-system login and session-establishment requirements of claim 1. EX1003, ¶[181]. However, neither Toya nor RFC 3261 explicitly discloses the mechanism by which the terminal provides a screen-capture program to the external device for automatic execution upon connection. Chang discloses this with its plug-and-show USB portable disk that automatically delivers green software from the conferencing hub system to a presenter’s laptop upon USB connection, causes the software to execute on the

laptop to capture presentation frame data, and forwards the captured data to the wireless gateway for display to remote conference participants—all without requiring pre-installation. EX1007, Abstract, 4:49-5:21; EX1003, ¶[181].

Chang's disclosures map directly to each limitation of claims 4–6 for the same reasons applicable to the Toya/Tucker/Chang combination. *See supra* §VII.B.2-5. For claim 4, Chang teaches that when the USB portable disk engages with the laptop, the auto-run plug-and-show program initiates a request for the laptop to permit execution of the image capturing and analyzing program (claim 4.a), and upon permission the program executes on the laptop to capture display data that is forwarded to the wireless gateway (claim 4.b). *See supra* §VII.B.2-3. For claim 5, Chang teaches that the hub system transmits the screen-capture program to the laptop via the USB portable disk upon connection. *See supra* §VII.B.4. For claim 6, Chang's green-software architecture satisfies the conditional-installation requirement because the program is never permanently installed on the laptop—it is loaded fresh upon each connection and removed upon disconnection—so the system necessarily transmits the program each time the connection occurs, precisely because the program is not present on the external device at the time of connection. *See supra* §VII.B.5; EX1003, ¶[182].

A POSITA would have been motivated to combine Chang with Toya and RFC 3261 because all three references address systems for sharing multimedia content

during conferences or communication sessions, because Chang directly solves the problem of enabling seamless screen sharing from external laptops without pre-installation (the identical problem identified in the '917 Patent's specification), and because the combination yields the entirely predictable result of a SIP-based video conferencing terminal that automatically provides a screen-capture program to a connected external device so that the device's display data can be captured and shared with remote conference participants over the established session. **The substitution of RFC 3261 for Tucker does not alter the motivation to combine Chang**, because how Chang is used—program delivery and automatic execution on the external device—is independent of whether the session-establishment authentication is taught by Tucker's server-mediated website authentication or by RFC 3261's SIP REGISTER and authentication mechanisms. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007); EX1003, ¶¶[183]-[190].

1. Motivation to Combine

A POSITA would have been motivated to incorporate Chang's plug-and-show program-delivery mechanism into the Toya/RFC 3261 combination for several independently sufficient reasons.

Same Field of Endeavor: Chang, Toya, and RFC 3261 are all directed to systems for sharing image or video content during conferences or meetings. EX1003, ¶[185]. Chang specifically addresses wireless presentation

systems in which “plural representatives with their own computers may present to show their presentation files pre-stored in their own computers” during a “presentation conference.” EX1007, 1:43-54. This is the same conference content-sharing scenario addressed by Toya, which discloses a video communication device that receives content data from external devices and transmits it to a counterpart device during a television conference session established using SIP protocols. EX1004, 16:51-17:26. RFC 3261 provides the underlying SIP protocol specifications—including session establishment, authentication, and registrar functions—that govern how conferencing sessions are initiated and secured. EX1006, Abstract, §22, §26.1.1. A POSITA designing a SIP-based video conferencing terminal with content-sharing capabilities from external devices would have naturally looked to Chang’s plug-and-show architecture to solve the problem of how to enable external laptops to share screen data without pre-installing software. EX1003, ¶[185].

Chang Solves a Problem That Toya and RFC 3261 Do Not Address: The Toya/RFC 3261 combination provides the foundational video conferencing architecture—including SIP-based session establishment, authentication via registrars, and content sharing from external devices through local interfaces—but does not explicitly address the software executed by an external device to enable sharing of content data, or how that software is made available to the external device.

Toya discloses that its video communication device receives content data from external sources (via Bluetooth, infrared, and Ethernet interfaces), but does not describe how the external device obtains the software necessary to share images or video. EX1004, 18:32-19:7. RFC 3261 addresses SIP signaling, authentication, and session management, but is silent on host-to-peripheral program deployment. EX1006, Abstract, p. 1, §22, §26.1.1; EX1003, ¶[186].

Chang directly solves this problem. Chang identifies the prior art deficiency—“a specific drive program for the wireless projector is needed to be installed into the computer prepared for a corresponding wireless projector”—and explains that requiring pre-installation causes presenters to “need to install a proper drive program immediately at the conference site,” which “may ruin his/her presentation or at least cost the conference flow.” EX1007, 1:32-65. Chang’s solution is a USB portable disk that stores green software (requiring no pre-installation) and, upon physical connection to the presenter’s laptop, automatically delivers and executes a screen-capture program that captures presentation frame data and forwards it to the conferencing gateway for display to all participants. EX1007, Abstract, 4:39-5:8. A POSITA would have been motivated to incorporate Chang’s plug-and-show program-delivery mechanism into the Toya/RFC 3261 combination to enable seamless sharing of media content from any external device connected to the conferencing terminal—without requiring that device to pre-install content-

sharing software or to independently authenticate with the SIP registrar. EX1003, ¶[187].

Chang’s Express Motivation: Chang expressly identifies the motivation for its approach: eliminating the need for pre-installation of drive programs on each presenter’s computer, avoiding time needed for the installation as well as the restart process that “may ruin his/her presentation,” and enabling presentation “any time after the plug-and-show USB portable disk is plugged into the computer.” EX1007, 1:32-2:9, 3:51-65. Chang further explains that “no new installation is required to each of the computers” and that “the presentation can be initiated any time after the plug-and-show USB portable disk 25 is plugged into the computer 23.” EX1007, 3:51-65. These same motivations apply directly to Toya’s content-sharing system: a SIP-based video conferencing terminal that can automatically provide screen-capture software to any connected external laptop—without requiring pre-installation or separate authentication—delivers the same plug-and-show convenience in the video conferencing context, while RFC 3261’s authentication mechanisms ensure that only the conferencing terminal (not the external laptop) must authenticate with the management system before establishing the session. EX1003, ¶[188].

Predictable Combination of Known Elements: The combination of Toya, RFC 3261, and Chang is the predictable use of known prior art elements according

to known methods to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007). Toya teaches a video conferencing terminal that receives content from external devices and forwards it over an established SIP-based session. EX1004, 16:49-17:26, 17:57-18:49, 19:28-20:32. RFC 3261 teaches SIP authentication via registrars and challenge-based mechanisms, ensuring that only authorized terminals participate in conference sessions. EX1006, §22, §26.1.1. Chang teaches delivering a screen-capture program from a conferencing hub (via a USB portable disk) to an external computer upon connection, with the program automatically executing on the external computer to capture and forward display data to the conferencing system—all without pre-installation. EX1007, Abstract, 4:49-5:8. Incorporating Chang's plug-and-show program-delivery mechanism into the Toya/RFC 3261 combination yields the entirely predictable result: when an external laptop connects to the SIP-authenticated video conferencing terminal, the terminal provides a screen-capture program to the laptop (via a USB dongle or equivalent physical mechanism), the laptop permits execution of the program, the program captures the laptop's display data, and the captured data is forwarded to the conferencing counterpart over the SIP-established session—with the external laptop never needing to independently register with or authenticate to the SIP registrar. EX1003, ¶[189].

Reasonable Expectation of Success: A POSITA would have had a reasonable expectation of success because Chang's plug-and-show architecture operates at the physical device-connection interface (USB engagement between an external computer and a conferencing hub), which is independent of the SIP signaling and authentication layer taught by Toya and RFC 3261. EX1003, ¶[190]. The modification requires no changes to the SIP session establishment, registrar authentication, or relay architecture—it merely adds Chang's program-delivery and auto-execution mechanism at the point where the external device physically connects to the terminal. EX1003, ¶[190]. The combination of SIP-based conferencing (Toya/RFC 3261) with USB-based plug-and-show content sharing (Chang) would have been a straightforward integration of two independently functioning subsystems operating at different layers of the system architecture. EX1003, ¶[190].

2. [4.a]/[11.a]

Chang discloses this element for the same reasons discussed in Section VII.B.2, *supra*, which is incorporated by reference. EX1003, ¶[191].

3. [4.b]/[11.b]

Chang discloses this element for the same reasons discussed in Section VII.B.3, *supra*, which is incorporated by reference. EX1003, ¶[192].

4. Claim 5/12

Chang discloses this element for the same reasons discussed in Section VII.B.4, *supra*, which is incorporated by reference. EX1003, ¶[193].

5. Claim 6/13

Chang discloses this element for the same reasons discussed in Section VII.B.5, *supra*, which is incorporated by reference. EX1003, ¶[194].

VIII. CONCLUSION

Petitioner respectfully requests institution of IPR and cancellation of all claims of the '917 Patent.

IX. MANDATORY NOTICES PURSUANT TO 37 C.F.R. §42.8

A. Real Parties-In-Interest under 37 C.F.R. §42.8(b)(1).

The real party-in-interest is Zoom Communications, Inc. No other parties exercised or could have exercised control over this Petition. No other parties funded or directed the filing of this Petition.

B. Related Matters Under 37 C.F.R. §42.8(b)(2).

The '917 Patent is asserted in *Ricoh Company, Ltd. v. Zoom Communications, Inc. f/k/a Zoom Video Communications, Inc.*, No. 25-2095 (JCG) (D. Del.).

C. Lead and Back-up Counsel under 37 C.F.R. §42.8(b)(3).

Amanda S. Bonner (Lead Counsel) Registration No. 65,224 MAYER BROWN LLP 71 South Wacker Drive	B. Clayton McCraw (Back-up Counsel) Registration No. 68,258 MAYER BROWN LLP 1221 Avenue of the Americas
--	--

Chicago, IL 60606 Telephone: (312) 701-8645 Facsimile: 312-701-7711 asbonner@mayerbrown.com	New York, NY 10020-1001 Telephone: (212) 506-2649 CMcCraw@mayerbrown.com Cliff A. Maier (Back-up counsel) Registration No. 59,526 Mayer Brown LLP 3000 El Camino Real Palo Alto, CA 94206-2112 Telephone: 650-331-2026 CMaier@mayerbrown.com Nicholas Ciulla (Back-up counsel) Registration No. 78,409 Mayer Brown LLP 71 South Wacker Drive Chicago, IL 60606 Telephone: (312) 701-7779 Facsimile: 312-701-7711 nciulla@mayerbrown.com
--	--

D. Service Information under 37 C.F.R. §42.8(b)(4).

Please direct all correspondence to lead counsel at the address identified above. Petitioner consents to electronic service on counsel of record.

X. GROUNDS FOR STANDING

Petitioner certifies that the '917 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review of the '917 Patent. 37 C.F.R. §42.104(a).

XI. PAYMENT OF FEES

A fee of \$51,875 charged to Deposit Account 130019 was paid with the filing this petition. 37 C.F.R. §§42.15(a), 42.103. Should any further fees be required by the present Petition, the Board is hereby authorized to charge the above-referenced Deposit Account.

XII. STATEMENT OF PRECISE RELIEF REQUESTED

Petitioner requests IPR and cancellation of claims 1-15 because they are unpatentable under 35 U.S.C. §103 based on the foregoing grounds.

Date: August 24, 2026

Respectfully submitted,

By:/ Amanda Streff Bonner /

Patent No. 10,931,917
Petition for *Inter Partes* Review

Amanda Streff Bonner (Reg. No. 65,224)
Nicholas Ciulla (Reg. No. 78,409)
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: 312-701-8645
Facsimile: 312-701-7711
asbonner@mayerbrown.com
nciulla@mayerbrown.com

B. Clayton McCraw
Registration No. 68,258
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2649
CMcCraw@mayerbrown.com

Cliff A. Maier
Registration No. 59,526
Mayer Brown LLP
3000 El Camino Real
Palo Alto, CA 94206-2112
Telephone: 650-331-2026
CMaier@mayerbrown.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6 and 42.105, I hereby certify that on August 24, 2026, a copy of the attached PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,931,917, together with all exhibits, and all other papers filed therewith, including a Power of Attorney on behalf of Petitioners, was served via Priority Mail Express on the attorneys of record for the patent owner at the following address:

Attorney of Record for Patent Owner

22850 - OBLON, MCCLELLAND, MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314
UNITED STATES

A courtesy copy was also sent via email to counsel of record in the corresponding litigation.

Date: August 24, 2026

Respectfully submitted,

By: / Amanda Streff Bonner /
Amanda Streff Bonner (Reg. No. 65,224)
Nicholas Ciulla (Reg. No. 78,409)
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: 312-701-8645
Facsimile: 312-701-7711
asbonner@mayerbrown.com
nciulla@mayerbrown.com

B. Clayton McCraw

Patent No. 10,931,917
Petition for *Inter Partes* Review

Registration No. 68,258
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2649
CMcCraw@mayerbrown.com

Cliff A. Maier
Registration No. 59,526
Mayer Brown LLP
3000 El Camino Real
Palo Alto, CA 94206-2112
Telephone: 650-331-2026
CMaier@mayerbrown.com

Counsel for Petitioner

CERTIFICATION PURSUANT TO 37 C.F.R. § 42.11

Pursuant 37 C.F.R. § 42.11, the undersigned certifies that this PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,931,917, and accompanying evidence are not being presented for an improper purpose and that all legal contentions, allegations, and denials are warranted and have evidentiary support.

Date: August 24, 2026

Respectfully submitted,

By:/ Amanda Streff Bonner /
Amanda Streff Bonner (Reg. No. 65,224)
Nicholas Ciulla (Reg. No. 78,409)
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: 312-701-8645
Facsimile: 312-701-7711
asbonner@mayerbrown.com
nciulla@mayerbrown.com

B. Clayton McCraw
Registration No. 68,258
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2649
CMcCraw@mayerbrown.com

Cliff A. Maier
Registration No. 59,526
Mayer Brown LLP
3000 El Camino Real
Palo Alto, CA 94206-2112

Telephone: 650-331-2026
CMaier@mayerbrown.com

Counsel for Petitioner

CERTIFICATION PURSUANT TO 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), the undersigned certifies that this PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,931,917 complies with the type-volume limitation of 37 C.F.R. § 42.24(a). The word count application of the word processing program used to prepare this paper states that the paper contains 13,847 words, excluding the parts of the paper exempted by 37 C.F.R. §§ 42.24(a)(1).

Date: August 24, 2026

Respectfully submitted,

By:/ Amanda Streff Bonner /
Amanda Streff Bonner (Reg. No. 65,224)
Nicholas Ciulla (Reg. No. 78,409)
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: 312-701-8645
Facsimile: 312-701-7711
asbonner@mayerbrown.com
nciulla@mayerbrown.com

B. Clayton McCraw
Registration No. 68,258
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2649
CMcCraw@mayerbrown.com

Cliff A. Maier
Registration No. 59,526
Mayer Brown LLP

3000 El Camino Real
Palo Alto, CA 94206-2112
Telephone: 650-331-2026
CMaier@mayerbrown.com

Counsel for Petitioner