

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Singh et al.
U.S. Patent No.: 8,904,030 Attorney Docket No.: 50048-0060IP1
Issue Date: December 2, 2014
App. Serial No.: 14/295,353
Filing Date: June 4, 2014
Title: AUTOMATIC MULTIMEDIA UPLOAD FOR
PUBLISHING DATA AND MULTIMEDIA CONTENT

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

**PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT
NO. 8,904,030 PURSUANT TO 35 U.S.C. §§ 311-319, 37 C.F.R. § 42**

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
	A. Standing.....	1
	B. Challenge and Relief Requested.....	1
II.	THE '030 PATENT	2
	A. Brief Description	2
	B. Summary of the Prosecution History	4
III.	LEVEL OF ORDINARY SKILL	5
IV.	CLAIM CONSTRUCTION	5
V.	THE CHALLENGED CLAIMS ARE NOT ENTITLED TO CLAIM PRIORITY TO ANY EARLIER FILING DATE	6
	A. Legal Standard.....	6
	B. No Challenged Claim is entitled to a priority date before June 4, 2014	8
VI.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	11
	A. GROUND 1A—Claims 1-2, 4-7, 9-18 are obvious over Hiroishi, Takahashi, and Bluetooth	11
	1. Hiroishi	11
	2. Takahashi.....	11
	3. Bluetooth	12
	4. The Predictable Combination of Hiroishi-Takahashi-Bluetooth	14
	5. Motivation to Combine with a Reasonable Expectation of Success...	15
	6. Analysis	20
	B. GROUND 1B—Claims 1-2, 4-7, 9-18 are obvious over Hiroishi, Kahn, and Bluetooth.....	51
	1. Kahn	51
	2. Hiroishi-Kahn-Bluetooth Combination.....	52
	3. The Predictable Combination of Hiroishi, Kahn, and Bluetooth.....	53
	4. Analysis	58
	C. Ground 2A—Claims 1-2, 4-7, 9-14 are obvious over Singh ¹²⁹ in view of Bluetooth	68

D. Ground 2B—Claims 15-18 are obvious over Singh129 in view of Bluetooth and Takahashi	78
VII. DISCRETIONARY CONSIDERATIONS	81
A. The <i>Advanced Bionics</i> Test Favors Institution—§325(d).....	81
B. The <i>Fintiv</i> Factors Favor Institution—§314(a)	82
VIII. PAYMENT OF FEES – 37 C.F.R. §42.103.....	83
IX. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	83
A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)	83
B. Related Matters Under 37 C.F.R. § 42.8(b)(2).....	84
C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	85
D. Service Information	85

LIST OF EXHIBITS

- TTI-1001 U.S. Patent No. 8,904,030 to Singh et al. (“the ’030 patent”)
- TTI-1002 Excerpts from the Prosecution History of the ’030 patent
- TTI-1003–1008 RESERVED
- TTI-1009 U.S. Patent App. Pub. No. 2009/0172129 to Singh et al. (“Singh129”)
- TTI-1010 U.S. Patent App. Pub. No. 2008/0103906 to Singh (“Singh906”)
- TTI-1011 Certified Translation of JP 2003-60953 (“Hiroishi”)
- TTI-1012 Certificate of Translation for Hiroishi
- TTI-1013 Original Japanese Publication of Hiroishi
- TTI-1014 Certified Translation of JP 2005-303511 (“Takahashi”)
- TTI-1015 Certificate of Translation for Takahashi
- TTI-1016 Original Japanese Publication of Takahashi
- TTI-1017 U.S. Patent App. Pub. No. 2004/0004737 to Kahn (“Kahn”)
- TTI-1018 RESERVED
- TTI-1019 Bluetooth™ Core Specification 2.1 + EDR (“Bluetooth”)
- TTI-1020–1029 RESERVED
- TTI-1030 Declaration of David Lett
- TTI-1031 Archived Webpage Bluetooth™ Core Specification v2.1 + EDR
(<https://web.archive.org/web/20071011031607/http://bluetooth.com/Bluetooth/Learn/Technology/Specifications/Default.htm>)

- TTI-1032 C. Bisdikian, "An overview of the Bluetooth wireless technology," in IEEE Communications Magazine, vol. 39, no. 12, pp. 86-94, Dec. 2001, doi: 10.1109/35.968817. ("The Bluetooth Overview")
- TTI-1033 RESERVED
- TTI-1034 Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) ("Interim Guidance")
- TTI-1035 TikTok Stipulation letter regarding IPR grounds in District court litigation
- TTI-1036 CellSpin Preliminary Infringement Contentions in *CellSpin Soft, Inc. v. ByteDance, Ltd. et al.*, Case No. 2:23-cv-496 (E.D. Tex.)

LISTING OF CLAIMS

Claim 1	
1.P	A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:
1.1	performing at a Bluetooth enabled data capture device:
1.2	establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;
1.3	sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;
1.4	acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;
1.5	detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:
1.6	receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;
1.7	receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;
1.8	enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

1.9	determining existence of the new data for transfer; and
1.10	sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;
1.11	encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and
1.12	transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.
Claim 2	
2.	The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.
Claim 4	
4.	The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

Claim 5	
5.	The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.
Claim 6	
6.P	A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:
6.1	performing at a Bluetooth enabled data capture device:
6.2	establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;
6.3	acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;
6.4	detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:
6.5	receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;
6.6	determining existence of the new data for transfer; and
6.7	creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a timestamp attribute inside the data object, wherein the data signal notification corresponds to existence of new

	data for transfer, and wherein the timestamp corresponds to a time when new data was acquired;
6.8	encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and
6.9	transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.
Claim 7	
7.	The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.
Claim 9	
9.	The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.
Claim 10	
10.	The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

Claim 11	
11.	The method of claim 6, wherein the timestamp is either absolute time or relative time.
Claim 12	
12.P	A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:
12.1	providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:
12.2	establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;
12.3	receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;
12.4	detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:
12.5.1	sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,
12.5.2	wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;
12.6	enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

12.7	receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and
12.8	sending a request to the Bluetooth enabled data capture device, to get new data for transfer;
12.9	receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and
12.10.1	transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and
12.10.2	wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.
Claim 13	
13.	The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.
Claim 14	
14.	The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.
Claim 15	
15.P	A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:
15.1	performing at a Bluetooth enabled mobile device:

15.2	establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;
15.3	detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:
15.4	sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device
15.5	enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;
15.6	receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and
15.7	sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and timestamp, and wherein the timestamp corresponds to a time when new data was acquired;
15.8	receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;
15.9	obtaining new data, data associated with new data and timestamp from the received encrypted data object using cryptographic encryption key; and
15.10	sending the obtained new data and the obtained timestamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web

	address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.
Claim 16	
16.	The method of claim 15, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.
Claim 17	
17.	The method of claim 15, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.
Claim 18	
18.	The method of claim 6, wherein the timestamp is either absolute time or relative time.

TikTok Inc. (“Petitioner”) petitions for *Inter Partes* Review of claims 1-18 (“the Challenged Claims”) of U.S. Patent No. 8,904,030 (“the ’030 patent”).

Notably, in IPR2019-00127 and IPR2019-00131, similar claims of related U.S. Patent No. 9,258,698 (“the ’698 patent”) were found unpatentable over the prior art, including the Hiroishi and Takahashi references presented here. Although the challenged claims of the ’030 patent recite at least one additional limitation (*e.g.*, an event notification and other obvious variants) the Challenged Claims are likewise not patentable.

I. REQUIREMENTS FOR IPR

A. Standing

Petitioner certifies that the ’030 patent is available for IPR and Petitioner is not barred from requesting IPR.

B. Challenge and Relief Requested

Petitioner requests IPR of the Challenged Claims on the grounds listed below. A declaration from David Lett (TTI-1030) supports this Petition.

Ground	Claims	Basis
1A	1-2, 4-7, 9-18	§103: Hiroishi in view of Takahashi and Bluetooth
1B	1-2, 4-7, 9-18	§103: Hiroishi in view of Kahn and Bluetooth
2A	1-2, 4-7, 9-14	§103: Singh129 in view of Bluetooth
2B	15-18	§103: Singh129 in view of Bluetooth and Takahashi

No challenged claim can claim priority before the filing date of the application that issued as the '030 patent because the priority documents fail to disclose the claimed subject matter (as will be explained in Section V). Therefore, Singh129 qualifies as prior art under AIA 35 U.S.C. § 102(a)(1). Singh129 published on July 2, 2009, many years before the filing of the application that issued as the '030 patent.

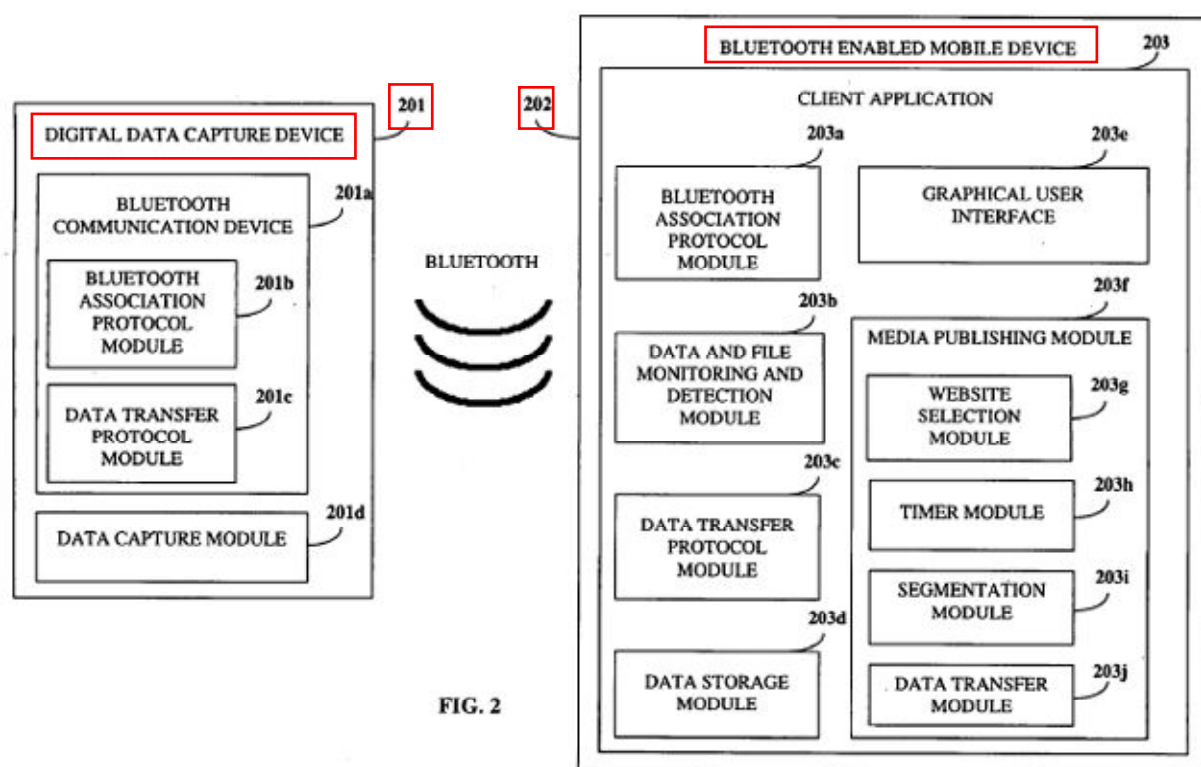
As shown below, each remaining reference pre-dates the '030 patent's earliest claimed priority date of December 28, 2007 (the alleged "Critical Date").

Reference	Publication Date	Prior Art At Least Under
Hiroishi	Feb. 28, 2003	Pre-AIA § 102(b)
Takahashi	Oct. 27, 2005	Pre-AIA § 102(b)
Kahn	Jan. 8, 2004	Pre-AIA § 102(b)
Bluetooth	July 26, 2007	Pre-AIA § 102(a)

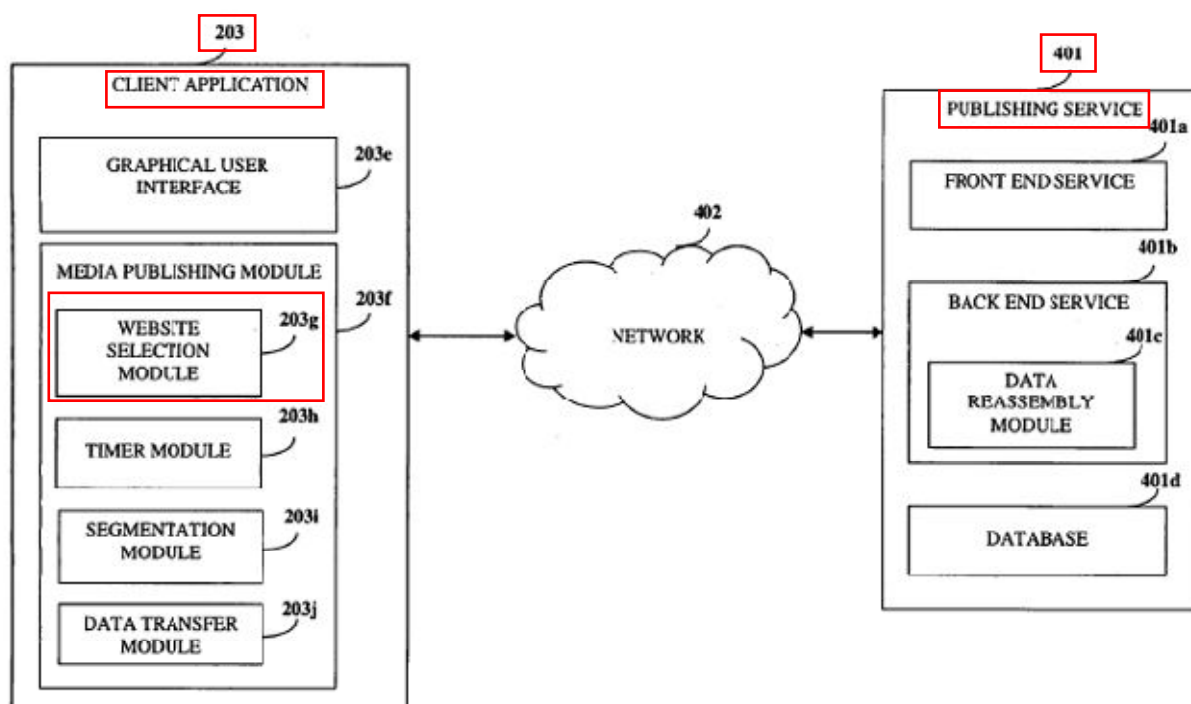
II. THE '030 PATENT

A. Brief Description

The '030 patent discloses "a method and system for utilizing a digital data capture device in conjunction with a Bluetooth (BT) enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention." TTI-1001, Abstract. As shown below, the '030 patent's system includes, among other things, digital data capture device 201, BT enabled mobile device 202, and publishing service 401. *Id.*, Figs. 2, 4.



Id., Fig. 2 (annotated).



Id., Fig. 4 (annotated).

As shown above, mobile device 202 includes client application 203, which “detects capture of data and multimedia content on the digital data capture device” and the “digital data capture device transfers the captured data, multimedia content, and the associated files to the client application.” *Id.*, Abstract. Then, the “client application automatically publishes the transferred data and multimedia content on one or more websites.” *Id.* Client application 203 includes, among other things, website selection module 203g. *Id.* “The website selection module 203g selects the websites based on settings and user preferences configured by the user on the mobile device 202.” *Id.*, 7:3-6.

B. Summary of the Prosecution History

U.S. Patent Application No. 14/295,353 (“the ‘353 application”) was filed on June 4, 2014. The examiner initially rejected all 20 claims citing non-statutory obviousness-type double patenting and 35 U.S.C. 103(a). TTI-1002, 72-73. In response, a terminal disclaimer was filed for the double patenting issue, while claims were amended to address the 35 U.S.C. 103(a) rejection. *Id.*, 36-44, 67. Amendments included additions related to “cryptographic encryption key” and “data signal notification.” *Id.* On October 3, 2014, a Notice of Allowance was issued, incorporating examiner’s amendments from a September 23, 2014 telephone interview, citing lack of prior art teaching or suggesting amended claims.

Id., 1-13.

III. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art (“POSITA”) at the time of the ’030 patent alleged Critical Date would have had at least a bachelor’s degree in electrical engineering, computer engineering, or computer science, and two years of experience in the field consumer electronics, with exposure to digital camera technology and wireless communications. TTI-1030, [94]-[95]. Superior education could compensate for a deficiency in work experience, and vice-versa.

Id.

IV. CLAIM CONSTRUCTION

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. § 42.100. Based on the well-established principal that “claim terms need only be construed to the extent necessary to resolve the controversy,” no express constructions are required to institute review and find the Challenged Claims unpatentable. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

Nonetheless, Petitioner notes that, for purposes of determining whether to institute IPR2019-00127 regarding related U.S. Pat. No. 9,258,698, the Board “determine[d] that ‘cryptographically authenticating identity of the cellular phone’ encompasses ‘authenticating the identity of the cellular phone using some form of

security or encryption, including by use of a shared passkey on the digital camera device and the cellular phone.” *Canon U.S.A., Inc. v. Cellspin Soft, Inc.*, IPR2019-00127, Paper 7, p. 11 (P.T.A.B. April 29, 2019); *but see id.* at Paper 51, pp. 17-18 (finding that no construction was required to address the patentability issues).

V. THE CHALLENGED CLAIMS ARE NOT ENTITLED TO CLAIM PRIORITY TO ANY EARLIER FILING DATE

The '030 patent claims priority, through a series of continuous applications, to a provisional application filed on December 28, 2007. '030 patent, Cover. However, no priority applications provide any indication that the inventors were in possession of the claimed combination of elements at issue here. TTI-1030, [101], [119]-[120]. Thus, no challenged claim can claim priority to an earlier filing date.

A. Legal Standard

To rely on the filing date of an earlier application, 35 U.S.C. § 120 requires that the earlier application include a disclosure that complies with the written description requirement of 35 U.S.C. § 112. *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1571-72 (Fed. Cir. 1997) (confirming the written description must provide more than that which “would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose”).¹ The written

¹ See *SAP Am., Inc. v. Pi-Net Int'l, Inc.*, IPR No. 2014-00414, Paper No. 11, 1114

description requirement is separate and distinct from the enablement requirement.

Ariad Pharm., Inc. v. Eli Lilly & Co., 598 F.3d 1336, 1340 (Fed. Cir. 2010) (*en banc*); *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1560 (Fed. Cir. 1991).

The written description requirement has several policy objectives. One objective is to convey to the public what the applicant claims as the invention. *See Regents of the Univ. of Cal. v. Eli Lilly*, 119 F.3d 1559, 1566 (Fed. Cir. 1997), *cert. denied*, 523 U.S. 1089 (1998). “[T]he disclosure as originally filed does not have to provide *in haec verba* support for the claimed subject matter at issue.” *Purdue Pharma L.P. v. Faulding Inc.*, 230 F.3d 1320, 1323 (Fed. Cir. 2000). However, “one skilled in the art, reading the original disclosure, must immediately discern the limitation at issue in the claims.” *Id.*

“The question is not a question of whether one skilled in the art might be able to construct the patentee’s device from the teachings of the disclosure ... it is a question whether the application necessarily discloses that particular device.” *Lockwood*, 107 F.3d at 1572.

(P.T.A.B. Aug. 18, 2014) (relying on § 112 case law is proper in an *inter partes* review to establish effective filing date).

**B. No Challenged Claim is entitled to a priority date before
June 4, 2014**

The Challenged Claims comprise four independent claims: 1, 6, 12, and 15.

Each of these claims have one or more of the following limitations:

- “performing at a Bluetooth enabled data capture device ... encrypting, using cryptographic encryption key, the new data [object] acquired in the Bluetooth enabled data capture device; and transferring the encrypted data [object] from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection ... wherein the Bluetooth enabled mobile device is configured to receive the encrypted data [object] and obtain the new data [and the data signal notification] from the encrypted data using cryptographic encryption key” (claims 1, 6)
- “receiving, by the Bluetooth enabled mobile device, encrypted data [object] corresponding to the new data [object] over the established Bluetooth paired secure wireless connection and obtaining new data[, data associated with new data and timestamp] from the received encrypted data [object] using cryptographic encryption key” (claims 12 and 15)
- “sending a message to the Bluetooth enabled mobile device [/

receiving a message from the Bluetooth enabled data capture device],
corresponding to supported data capability of the Bluetooth enabled
data capture device” (claims 1 and 12)

- “wherein new data object comprises of new data, data associated with
new data and timestamp, and wherein the timestamp corresponds to a
time when new data was acquired” (claim 15)

TTI-1030, [119]-[120]; *see also Canon*, IPR2019-00127, Paper 51, p. 12 (finding
that the specification of the ’698 patent, which is identical to the specification of
the ’030 patent, does not mention encrypted data exchange using the paired
connection).

The ’030 patent issued from an application filed on June 4, 2014. Although
the ’030 patent purports to be a continuation of and claims priority to several
earlier applications, claims 1-18 were not “disclosed in the manner provided by
section 112(a)” in any priority application, as required by 35 U.S.C. § 120, and
thus cannot claim the benefit of the filing date of the earlier application. *See*
Reiffin v. Microsoft Corp., 214 F.3d 1342, 1346 (Fed. Cir. 2000) (“In accordance
with § 120, claims to subject matter in a later-filed application not supported by an
ancestor application in terms of § 112 ¶ 1 ... do not receive the benefit of the
earlier application’s filing date.”); TTI-1030, [119]-[120].

In particular, the priority applications contains no written description of a data capture device encrypting acquired data or transferring encrypted data to a mobile device of a Bluetooth connection and thus no written description of a mobile device receiving/obtaining encrypted data from the data capture device. Rather, the priority applications merely describe a Bluetooth pairing process and transferring data over a Bluetooth connection. Notably, data encryption was an optional feature of Bluetooth at the time of the claimed invention. TTI-1030, [119]-[120]; TTI-1019, 1038. Similarly, no priority application contains a written description of sending/receiving a message corresponding to supported data capability of the Bluetooth enabled data capture device. TTI-1030, [119]-[120]. And no priority application contains a written description of a new data objection comprising a timestamp corresponding to a time when new data was acquired. *Id.*

Accordingly, no challenged claim can claim priority to an earlier application. *See Arthrex, Inc. v. Smith & Nephew, Inc.*, 35 F.4th 1328, 1344 (Fed. Cir. 2022) (confirming the Board's statutory authority to decide whether priority applications meet the written description requirement for the purpose of determining whether a reference is prior art).

VI. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A—Claims 1-2, 4-7, 9-18 are obvious over Hiroishi, Takahashi, and Bluetooth

1. Hiroishi

Hiroishi is a Japanese patent application published on February 28, 2003 and assigned to Fuji Photo Film Co., Ltd. Hiroishi, Face. Hiroishi qualifies as prior art under pre-AIA 35 U.S.C. § 102(b). TTI-1030, [122].

Hiroishi teaches a system that allows users to use a mobile phone to control a digital camera remotely. TTI-1011, Abstract, [0043]. In addition, Hiroishi discloses a “two-way wireless communication” using Bluetooth. *Id.*, [0066].

In one embodiment, a release instruction is issued by the mobile device, which in turn causes the camera to acquire and store new photographs. TTI-1011, [0078]. Once at “step 104,” the mobile device may then instruct the digital camera to transmit the stored image data to the mobile device. *Id.*, [0084]. The camera may also transmit a thumbnail of the image to the mobile device. *Id.*, [0081]. Once received, the mobile device may then upload it to another computing device. *Id.*, [0044].

2. Takahashi

Takahashi is a Japanese patent application published on October 27, 2005. Takahashi, Face. Takahashi qualifies as prior art under pre-AIA 35 U.S.C. § 102(b).

Takahashi teaches the use of mobile devices using HTTP to upload captured image data to remote servers immediately after captured in order to publish and share it on a user media publishing website. *See, e.g.*, TTI-1012 , [0020], [0062]; *see also id.*, Abstract, [0049], [0052], [0037]. A user ID is also uploaded along with the image data to identify the user. *Id.*, [0066]. Once received, the image storage server processes (e.g., resizes) the image prior to publishing the image to a webpage. *Id.*, [0052]. The user can choose what images to publish and share. *Id.* [0063].

3. Bluetooth

As of the alleged Critical Date, Bluetooth wireless technology (BT), had established its role in replacing cables for personal device interconnectivity and facilitating spontaneous communication between devices within a localized “communications bubble.” TTI-1032, 1-2. TTI-1019, 1, 89, 126. “Connecting to data services through one’s cellular phone gives rise to the concept of a personal gateway. People will carry their personal gateways wherever they go.” TTI-1032, 1. The Bluetooth specification details security implementation at both link and application layers, with cryptographic authentication through LMP Pairing and Secure Simple Pairing methods. *See, e.g.*, TTI-1019, 131, 1260. Cryptographic authentication was routine pre-dating the patent’s Critical Date. TTI-1019, 412. Bluetooth’s packet format allows flexible payload transportation, enabling image

transfer. TTI-1019, 293. Event listening/notification mechanisms like polling and sniff mode are defined in the Bluetooth specification. TTI-1019, 331-332, 345.

Bluetooth technology was available before the critical date of the patent, as supported by various pieces of evidence. TTI-1019, 1; TTI-1030, [47]-[60]. First, the face of the Bluetooth Core Specification V2.1 provides publication date as July 26, 2007. Second, the same Bluetooth Core Specification V2.1 was provided as an exhibit by the Patent Owner in two IPR proceedings (IPR2019-00127 as Ex. 2018 and IPR2019-00131 as Ex. 2006), both involving U.S. Patent 9,258,698 (a family member of the '030 patent). Third, the WayBack Machine contains an archived webpage in October, 2007, confirming the publication of the Bluetooth Core Specification V2.1 on July 26, 2007, and its public accessibility by no later than October, 2007. TTI-1031, 1. The content of the page is credible as it mentions Bluetooth 2.1 as the latest available release and thus predates the release of Bluetooth 2.2.

Bluetooth®

Learn

- Benefits of Bluetooth Technology
- > How Bluetooth Technology Works
- Bluetooth Technology
- Core Specification v2.1 + EDR
- Specification Documents
- Compare with Other Technologies
- Ultra Low Power Bluetooth Technology
- > Security
- Glossary
- Connect
- Apply
- About the Bluetooth SIG
- Press & Analysts

Select Language ▾

search site enter keywords here search >

Specification Documents

Bluetooth Technical Specification documents are made available in Adobe Acrobat format (PDF). If you have an idea for a new use case or for specification enhancements, please email Member Relations.

For proper viewing, you must use Adobe Acrobat version 6.0 or higher. This software can be downloaded here at no cost. Files over 2MB in size are compressed in .ZIP file format.

Items 1 - 15 of 47

Items per page: 15 ▾

Page 1 2 3 4

Bluetooth Core Specifications	Publish Date
Core Specification v2.1 + EDR	26-Jul-2007
Core Specification v2.0 + EDR	10-Nov-2004

TTI-1031, 1 (annotated). Finally, the '030 patent relies on pre-existing Bluetooth

technology and thus acknowledges that Bluetooth is prior art. TTI-1001, 2:3. *See, e.g.*, 1030, [47]-[60].

4. The Predictable Combination of Hiroishi-Takahashi-Bluetooth

In the proposed combination, as described by Hiroishi, a photograph system includes a cellular phone that connects to a camera via a Bluetooth connection. TTI-1012, [0066]-[0067], FIG. 1. The cellular phone controls the camera to capture images, store images, and transmit images to the cellular phone. *Id.* The cellular phone then transmits images to a remote computer destination by a cellular network connection via the Internet. *Id.* The mobile phone is configured to apply an action setting that leverages HTTP to the received images from the camera, in a manner similar to what was suggested by Takahashi. TTI-1030, [140]. Also in the combination, a user identifier is sent with the transmission of the images, similar to the image file name described by Takahashi. *Id.* And, a timestamp is sent revealing when the image or images were taken, in a manner similar to what was suggested by Takahashi. *Id.*

In addition, in the combination, based on Hiroishi, the Bluetooth-enabled camera encrypts the image data transmitted to Bluetooth-enabled cellular phone over the Bluetooth connection using an encryption technique consistent with the teachings of the TTI-1019. *Id.*, 141. Also similar to Hiroishi and as further

described by the Bluetooth Core Specification V2.1, in the combination, the camera provides a message corresponding to supported device capabilities to the mobile phone (e.g., after a Bluetooth connection has been established). *Id.*

5. Motivation to Combine with a Reasonable Expectation of Success²

A POSITA at the time of the invention would have been motivated to combine the teachings of Hiroishi, Takahashi, and Bluetooth, thus rendering the subject matter of the '030 patent challenged claims (1-2, 4-7, 9-18) obvious. TTI-1030, [142]-[159].

The combination of Hiroishi and Takahashi

Both Hiroishi and Takahashi are analogous art to the claimed invention, operating in the same field of endeavor: wireless image transfer from one electronic device to another. *Id.*, 143. Hiroishi teaches techniques for enabling a mobile device to control a digital camera and transfer image files and instructions between the two devices. TTI-1011, Abstract, [0066]. Takahashi is directed to wirelessly transferring image files from a mobile device to a publishing website

² The PTAB has already accepted that it would have been obvious to combine Hiroishi with Takahashi, for at least some of the reasons articulated above. *See, e.g.*, IPR2019-00127, Paper 1, 51-53, Paper 7, 30-34.

over the Internet with an action setting using HTTP. TTI-1014, Abstract, [0049], [0051], [0054].

Hiroishi and Takahashi are also pertinent to the problem of the '030 patent: transmission of image data by a cellular phone that was captured by a digital camera. TTI-1001, Background. Hiroishi addresses this problem through Bluetooth wireless data transmission and software-based control of the digital camera from the mobile device. *See, e.g.*, TTI-1011, [0043], [0053], [0061]; TTI-1030, [144]. Takahashi addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g.*, TTI-1014, [0049], [0071]; TTI-1030, [144].

A POSITA would have been motivated to use Takahashi's upload technique to publish image data received at the mobile device of Hiroishi. TTI-1030, [145]-[146]. At the time of the Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g.*, TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server). Takahashi recognizes both of these trends and teaches an efficient and predictable technique for uploading image data from a mobile device to a publishing website. *See, e.g.*, TTI-1014, Abstract; TTI-1030, [145]-[146].

The teachings of Takahashi would have provided straightforward benefit to the user of the mobile device in Hiroishi: the ability to upload image files and an

action setting to a publishing server using an existing HTTP connection between the mobile device and the publishing server. TTI-1014, [0071] (HTTP transmission instruction); TTI-1030, [147]; TTI-1011, [0044]. Takahashi would have furthered this purpose by allowing the user to transfer image data to additional locations. TTI-1030, [147].

A POSITA would have been motivated, and found it obvious, to include user identifier that uniquely identifies a particular user of the Internet service as taught by Takahashi. TTI-1030, [148]; TTI-1011, [0110]. If desired, a POSITA would have found it obvious to also include the user identifier with the images when transferring the images to the remote internet server. TTI-1030, [148]; *see also* TTI-1014 (Takahashi), [0055], [0066] (“user ID in the file name of image data.”) This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., by the file name, as taught by Takahashi. TTI-1030, [148]; *see also* TTI-1011, [0110]-[0113].

A POSITA would have also found it obvious to modify Hiroishi to include a timestamp with the images, in a manner similar to that suggested by Takahashi. TTI-1014, [0070]; TTI-1030, [149]. A POSITA would have recognized that including a date and time of when the images were captured would provide additional contextual information to the images. *Id.* In addition, adding a timestamp to the image file name would also uniquely identify the image file, and

allow sorting and organization in an album. *Id.* A POSITA would have found it obvious to modify the image file names of Hiroishi for at least these reasons. *Id.* Adding a timestamp to the file names of the images would have been well within the skill of a POSITA at the time. *Id.* As described by Takahashi, the time and date (to the second) could have been derived from an internal clock. *Id.*; TTI-1014, [0070]. Even though as Takahashi's internal clock is in the phone and transmitted to the camera, a POSITA would understand that a more accurate time stamp would be at the camera when the camera takes the picture, so it would have been obvious to add time stamp at the camera. It was also typical as of the alleged Critical Date to have a picture's time stamp added by digital camera. TTI-1017, [0008], [0060].

The combination of Hiroishi-Takahashi and Bluetooth

A POSITA would have found it obvious that the camera of Hiroishi would have provided a message corresponding to supported data capability of the camera to the mobile phone upon establishment of the Bluetooth connection, in a manner consistent with the protocols described in the Bluetooth Core Specification. TTI-1019 (Bluetooth Core Specification V2.1), 441-442 (4.3.4 Supported Features), 384-392 (3.2 Feature Definitions); TTI-1030, [152].

In addition, the reporting by the camera of supported data capability includes whether the camera supports encryption, which provides enhanced security and

was desirable. *Id.*; TTI-1019, 384-389; TTI-1030, [153]. An example of supported features in Bluetooth are summarized in Section 3.2 of the Bluetooth specification. TTI-1019, 133-135, 384-389; TTI-1030, [155]; TTI-1011, [0066]-[0067].

A POSITA would have also found it obvious to encrypt the image data transferred from the Bluetooth-enabled camera to the cellular phone of Hiroishi to provide enhanced security. TTI-1030, [156]-[157]. The Bluetooth Core Specification 2.1 describes the encryption of payload data. *Id.*; TTI-1019, 1038. Specifically, the Bluetooth Core Specification 2.1 states that “user information can be protected by encryption of the packet payload.” TTI-1019, 1038. For example, the “encryption of the payload shall be carried out with a stream cipher called E0 that shall be re-synchronized for every payload.” *Id.*

Reasonable expectation of success

There would have been a reasonable expectation of success in combining the teachings of Hiroishi and Takahashi and Bluetooth. TTI-1030, [158]-[159]. The combination would have required simply packaging the image data from the mobile device of Hiroishi in an HTTP message as Takahashi teaches and as what well known at the time for packet data transfer over the Internet. *Id.* Both modifications would have been well within the ability of a POSITA. *Id.*

The Bluetooth Core Specification 2.1 also teaches how to activate

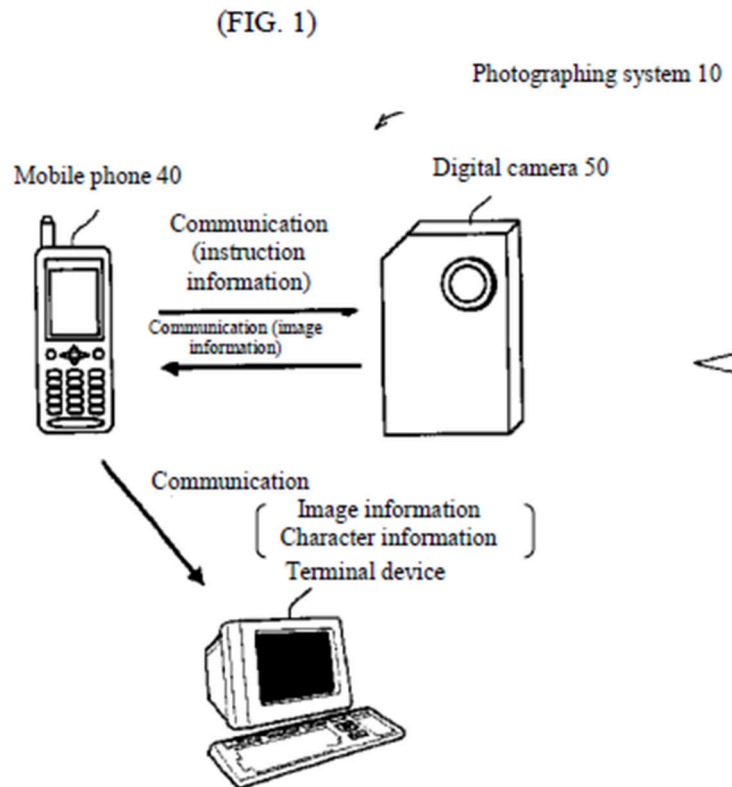
encryption between two Bluetooth devices (*see, e.g.*, TTI-1019, 882-884 (“Set Connection Encryption”)), as well as how to perform encryption to protect the payload. TTI-1019, 919 (“1 ENCRYPTION SAMPLE DATA”). For example, the Bluetooth Core Specification 2.1 suggests a “Massey and Reuppel method.” *Id.*, 1038, 1044-1056 (providing examples of how encryption can be implemented).

6. Analysis

[12.P]

To the extent the preamble is limiting, the Hiroishi-Takahashi-Bluetooth combination renders obvious [12.P]. TTI-1030, [160]-[168]. For example, Hiroishi’s system enables users to reliably capture self-portraits. Hiroishi, [0004]. *Id.*; TTI-1011, [0042], [0061], [0066]-[0068]. Hiroishi teaches a digital camera device 50. TTI-1011, Fig. 1, Abstract (“[a] digital camera 50...”). Hiroishi further teaches a cellular phone 40 with access to the internet. *Id.*, Fig. 2 (showing “mobile phone 40” connected to “Internet 12”), [0048], [0049]. Hiroishi further teaches that the digital camera is connected to the cellular phone over a wireless connection, such as Bluetooth. *Id.*, [0066], Fig 1. Hiroishi teaches a mobile phone (***Bluetooth enabled mobile phone***) to communicate (via Bluetooth) with a digital camera, transferring photos to a remote server via cellular network connection. *Id.*

In FIG. 1, Hiroishi illustrates a “basic configuration of the photographing system 10.” TTI-1011, [0126].

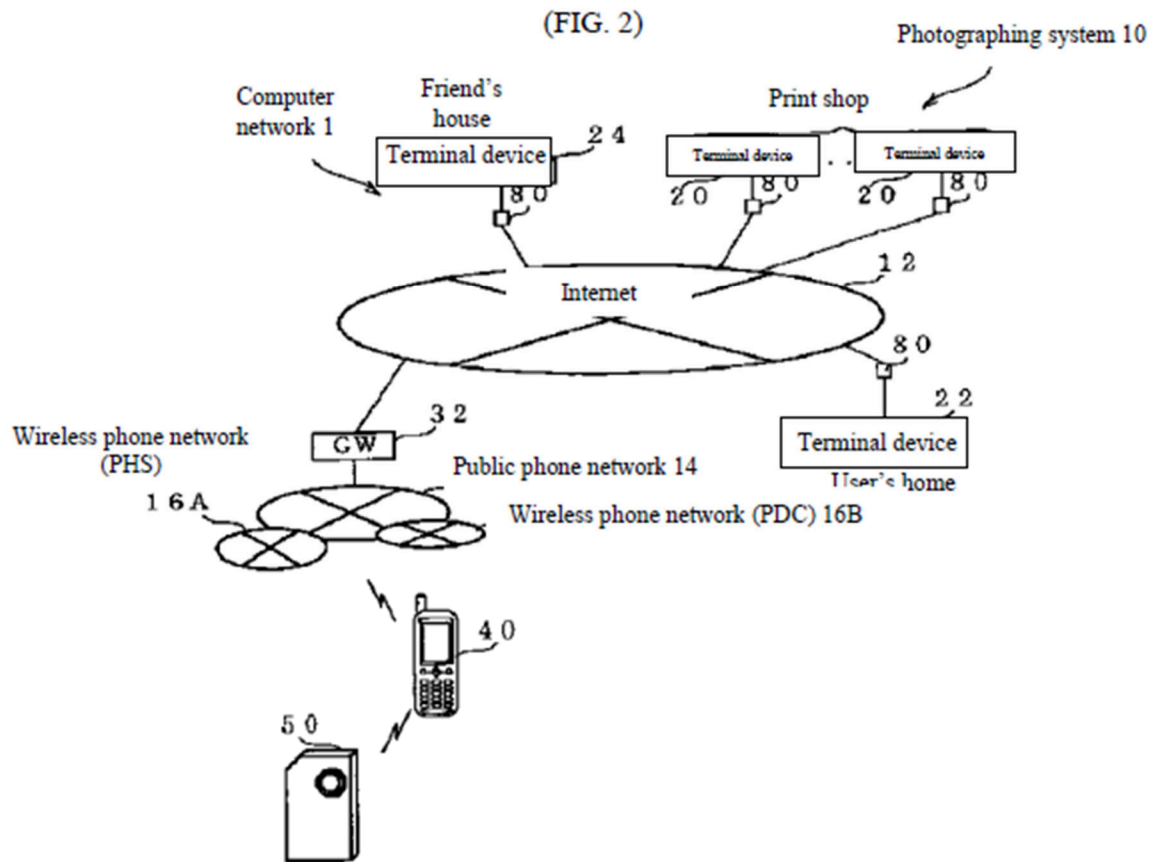


Hiroishi teaches that the mobile phone 40 is designed to connect with a CPU responsible for its operations, a ROM for storing control programs, and a RAM for temporary storage during program execution. TTI-1011, [0051].

Hiroishi teaches “[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed.” TTI-1011, Claim 10. Hiroishi lists the various instructions that the Bluetooth enabled cellular phone can send to the digital camera over the Bluetooth connection to control the digital camera. *Id.*, [0068]-[0069].

In FIG. 2, Hiroishi illustrates “the photographing system 10” connected to a “computer network 1” through “internet 12”. TTI-1011, [0046]-[0048], FIG. 2,

Abstract.



Id., FIG. 2.

In Fig. 2, the terminal devices 20, 22, and 24, are computers within the computer network 1, each connected to a network, enabling remote access by the cellular phone. TTI-1011, [0047]. A POSITA would recognize these terminals as remote servers as claimed. TTI-1030, [166]. Note that the term “remote server” is not defined by the '030 patent specification. At best, the '030 patent describes a publishing service connected to a network. TTI-1001, 7:29-51, FIG. 4. Hiroishi teaches the terminal devices 20, 22, 24 are likewise connected to a network (the

Internet), making them computers that are remotely accessible to the cellular phone. TTI-1030, [166]; TTI-1011, [0047]-[0049]. As an example, the terminal device 20 includes a computer at a print shop, which is a publishing service. *See, e.g.*, TTI-1011, [0049]; *see also id.*, [0049], [0105] (friend's computer).

Hiroishi's mobile phone 40 transfers data (via Bluetooth) to a terminal device (for example, *a remote internet server*) using a cellular network. TTI-1011, [0048]. Hiroishi teaches the telephone network includes a "Personal Digital Cellular" system. *Id.* The wireless telephone networks 16A and 16B can provide "transmission and reception functions of data to a mobile phone 40." *Id.*

[12.1]

See Ground 1A, [12. P]. The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.1]. TTI-1030, [169]-[172]. The Hiroishi teaches a software module (Hiroishi's "control programs" or "program that controls the operation of the camera" as modified by Takahashi) on the Bluetooth enabled mobile device (mobile phone 40). *See, e.g.*, TTI-1011, [0001], [0004], [0051], Claim 10; TTI-1030, [169].

A POSITA would have understood that Hiroishi's program would be an alternative term for the software module. TTI-1030, [170]. A POSITA would have understood that the mobile phone 40 would have implemented the software module to execute the program (or set of instructions). *Id.*

Hiroishi lists the various instructions that the Bluetooth enabled cellular phone can send to the digital camera over the Bluetooth connection to control the digital camera. TTI-1011, [0068]-[0069]; TTI-1030, [172].

[12.2]

The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.2] per the Bluetooth specification. TTI-1030, [173]-[180]. For example, Hiroishi teaches a two-way communication between a phone and a camera via Bluetooth to “perform transfer of data signals.” TTI-1011, [0066]-[0067]. In FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. *Id.*, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth connection. *Id.*; *see also id.*, [0070], [0074]-[0088], [0091]-[0107], [0121].

To the extent the Patent Owner argues that Hiroishi does not expressly disclose that the Bluetooth pairing between the cellular phone and the digital camera includes using a cryptographic encryption key, it would have been obvious to a POSITA to modify Hiroishi to include this limitation. TTI-1030, [170]-[180]. The use of such cryptographic encryption keys was a standard and well known part of the Bluetooth specification. *Id.*; TTI-1019, 410-417. For example, as discussed in the TTI-1019, pairing between Bluetooth devices includes the generation and exchange of initialization keys created from a PIN, a random number, and a

Bluetooth Device Address (BD_ADDR). TTI-1019, 410-417. Referring to Bluetooth Core Specification 2.1 (July 2007), the pairing processes uses the BD_ADDR to form the initialization key (Kinit). TTI-1019, 410-417 (Pairing).

Additionally, the Bluetooth Core specification describes the process for establishing a secure pairing as well as the obvious reasons behind secure pairing such as the prevention of eavesdropping. *Id.*, 131-132 (Secure Pairing).

The Bluetooth Core Specification describes implementation of security at both the link layer and the application layer. TTI-1019, 1025-1037 (Security Overview).

Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. TTI-1030, [47]-[60], [170]-[180]. Indeed, cryptographic authentication was part of Bluetooth for years before the priority date of the '030 Patent. *Id.*

A POSITA would have understood the basic motivation for using cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. TTI-1030, [170]-[180]. A POSITA would have found this benefit directly applicable to the system disclosed Hiroishi, because it would have ensured the secure transmission of image files and related data between the two devices. *Id.*

[12.3]

The Hiroishi-Takahashi-Bluetooth-Kahn combination renders obvious step [12.3] per the Bluetooth specification. TTI-1030, [181]-[183]. The Hiroishi-Takahashi-Bluetooth combination's software module on the Bluetooth enabled mobile device is configured to perform the step of receiving a message (LMP_features_res) from the Bluetooth enabled data capture device (Hiroishi's digital camera 50), corresponding to supported data capability of the Bluetooth enabled data capture device. *Id.* Indeed, the Hiroishi-Takahashi-Bluetooth combination's Bluetooth connection between the mobile phone 40 and digital camera 50 complies with the Bluetooth protocols available in 2007, which described the exchange of supported features between the Bluetooth devices. *Id.*; TTI-1019, 441, 133 (Association Models).

As shown in the cited pages, the ***max supported page*** is indicative of supported data capability of the Bluetooth enabled mobile device. *Id.*; TTI-1030, [182]. Other examples of features that are reported include number of slots per packet (3 slot packets or 5 slot packets), Adaptive Frequency Hopping (AFH) capability, Channel Quality Driven Data Rate, and Enhanced Data Rate (EDR). TTI-1019, 384-392 (explaining feature definitions). TTI-1030, [182].

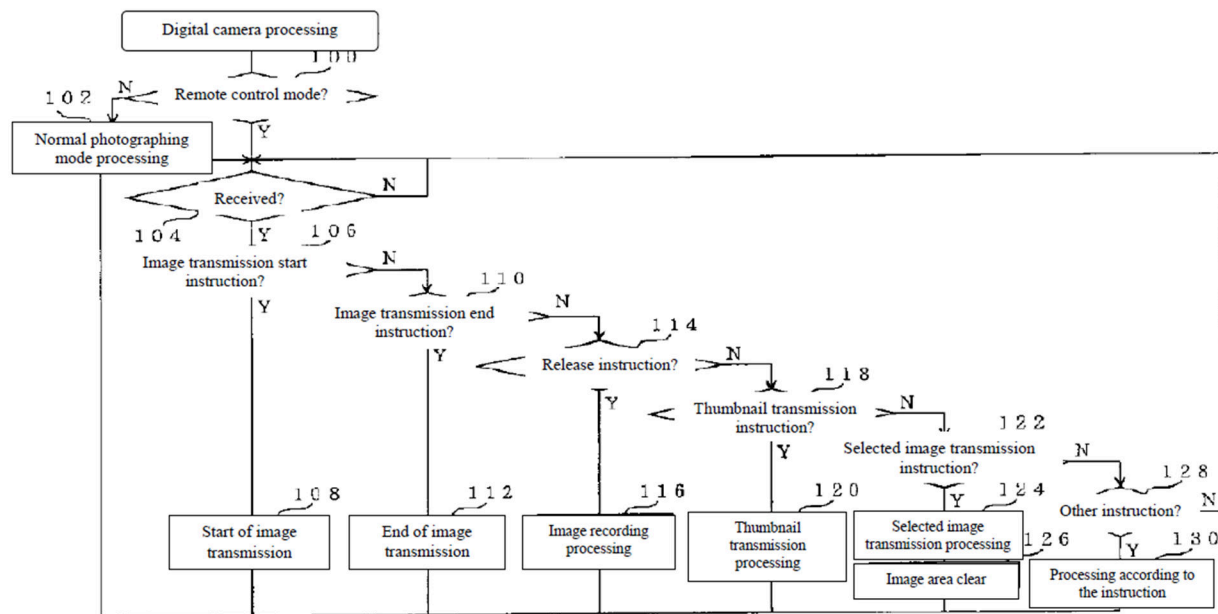
It would have been obvious to use this supported data functionality in the combination because it is essential to match the supported data capability of the

Bluetooth-enabled devices. *Id.*, [183].

[12.4]

The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.4]. TTI-1030, [184]-[187]. For example, Hiroishi teaches detection of new-data by sending a “release instruction” from the cellular phone 40 to the digital camera 50 after establishing a Bluetooth connection between the camera and the phone. TTI-1011, Abstract, [0012]. Hiroishi emphasizes that “the release instruction information is the information for instructing the timing of photographing with the camera.” *Id.*, [0034]. *Id.*

(FIG. 5)



TTI-1011, FIG. 5.

As shown above in FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. TTI-1011, FIG. 5, [0071]-[0078]. In steps 100 and

104, the camera determines whether it is under remote control of the phone via the Bluetooth. *Id.* At step 114, the camera receives a release instruction from the phone causing it to acquire a new image. *Id.*, Abstract, [0034], [0078]. A POSITA would understand that, because the release instruction is received from the phone over the Bluetooth connection, the image is acquired after the wireless connection is established. TTI-1030, [186].

In summary, a POSITA would have understood that the combination's software module on the mobile device detects new data acquired because when 1) the user sends a "release instruction" to the camera, resulting in the camera storing a captured image in its memory; 2) the user instructs the camera to end image transmissions; 3) the camera generates thumbnail images of the images stored in memory; and 4) the cellular phone receives the thumbnail images. The reception of the thumbnail images is the **detection** of new-data acquired. (emphasis added). TTI-1030, [187].

[12.5.1]

See Ground 1A, [12.4].

The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.5.1]. *See, e.g.*, TTI-1030, [188]-[196]. In the claim, the cellular phone receives an event notification signal to inform the cellular phone of the existence of new data. In the Hiroishi-Takahashi-Bluetooth combination, there are a variety of

signals that would perform the event notification function. For example, Hiroishi sends thumbnails to the cellular phone. TTI-1011, [0081]-[0082]. Upon receipt of the thumbnails, the cellular phone is notified that the pictures represented by the thumbnails are available. *See, e.g., id.*, [0105], FIG. 7C.

It would have been obvious to include header information, metadata, or some other information with the thumbnails or in addition to the thumbnails that informs the cellular phone of the nature of the received data—that new photos are available. TTI-1030, [191]. A person of ordinary skill would have reason to provide an event notification or designate pre-existing data as an event notification so that the cellular phone is made aware that new data is available so that it may then take appropriate actions in response. *Id.* Because thumbnails provide a straight-forward event notification to the user, a person of ordinary skill would further use the thumbnails or associated metadata as an event notification in the software running on the cellular phone. *Id.*

For example, Hiroishi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images). The mobile phone sends an instruction to the camera to transmit thumbnail images of the captured images stored on the camera's memory. *See* Ground 1A, [12.4]; TTI-1030, [192]. Specifically, Hiroishi teaches the following instructions that are sent from the mobile phone to the camera. TTI-

1011, [0068]. Hiroishi teaches the transmission end instruction information as the directive to cease the transmission of digital image data initiated by the image transmission start instruction information. *Id.* Additionally, it elucidates thumbnail transmission instruction information as the directive to transmit image data displaying the thumbnail of the image stored in SDRAM 55A. *Id.* A POSITA would have understood that Hiroishi exemplifies the facilitation of event notifications in the context of image transmission. *Id.*, [0068]; TTI-1030, [192]. Specifically, Hiroishi signifies the transition from viewfinder mode to transmission mode, allowing images to be sent as thumbnails in accordance with the transmission instructions provided. TTI-1011, [0068]. Hiroishi discloses that after the mobile phone sends a thumbnail transmission instruction to the camera, the camera processes images stored in memory (i.e., the new data) to create thumbnails, and sends the thumbnails to the mobile phone. *Id.*, [0081]-[0082].

Hiroishi teaches the thumbnails are then “transmitted according to the thumbnail transmission instruction information” to the mobile phone 40. *Id.*, [0067], [0084]. Thus, the mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable event notifications corresponding to the new data. TTI-1030, [192]-[194]. The full-resolution images stored in memory are the “new data,” and therefore, the thumbnails are notifications of the capture of the new data. *Id.* Likewise, the thumbnails “correspond” to the new data because

the thumbnails are a lower resolution representation of the full-resolution captured images stored in memory on the camera. *Id.*

Another example of sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data is disclosed in the Bluetooth Core Specification, by utilizing Sniff mode. Sniff mode is used to reduce power during an idle asynchronous connection as an alternative to constantly polling. TTI-1030, [195]-[196]; TTI-1019, 345.

There is a clear process for enabling event listening using sniff mode. TTI-1030, [195]-[196]; TTI-1019, 457.

[12.5.2]

Hiroishi-Takahashi-Bluetooth render [12.5.2] obvious. *See, e.g.*, TTI-1030, [197]-[198]. Because the new data (full resolution image) is obtained in response to instructions received by the digital camera 50 from the mobile phone 40 over the Bluetooth connection, the new data is acquired by the Bluetooth enabled data capture device (digital camera 50) after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device (digital camera 50) and the Bluetooth enabled mobile device (mobile phone 40). *Id.*; TTI-1011, [0078] (release instruction instructs image capture).

Hiroishi teaches that the mobile phone 40 and the digital camera 50 are

connected by a Bluetooth connection. TTI-1011, [0066]-[0067], [0121]. Further, Hiroishi discusses all of the instructions transmitted to and images received from the camera. *Id.*, [0068], [0073]-[0088]; *see also id.*, [0091]-[0107], [0121]; TTI-1030, [197]-[198].

[12.6]

The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.6]. TTI-1030, [199]-[202]. In the Hiroishi-Takahashi-Bluetooth combination, the detecting step (*see* Ground 1A, [12.4]) includes enabling event notification listening (activating the mobile phone code that “waits” to receive thumbnail images from the camera) on Bluetooth enabled mobile device, to listen (“wait”) for event notifications (thumbnail images) sent from the Bluetooth enabled data capture device (digital camera 50), over the established paired secure Bluetooth connection. *Id.* *See also*, Ground 1A, [12.5.1] (sniff mode).

As discussed above (*see* Ground 1A, [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone “waits” to receive the thumbnails from the camera. TTI-1030, [199]-[202]. A POSITA would recognize this “waiting” is the mobile phone listening for the event notifications (the thumbnails). *Id.*; TTI-1011, [0102], [0104]. This “waiting” is the mobile phone listening for event notifications. TTI-1030, [199]-[202]. A POSITA would understand that the term “waiting” (in step 230) in the context of

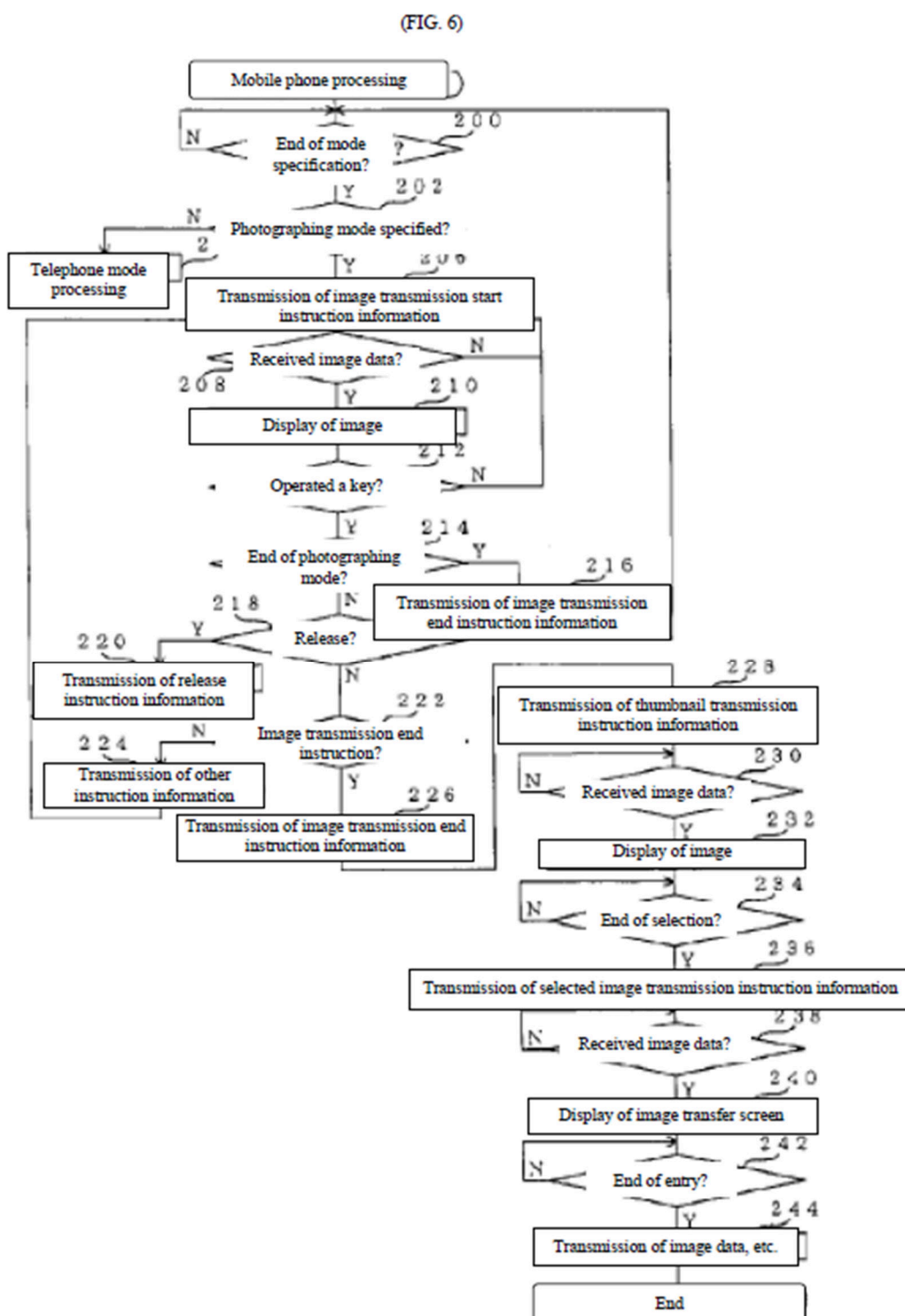
the mobile phone's action after sending a thumbnail transmission instruction to the camera implies a state where the mobile phone is actively listening for event notifications, particularly for the receipt of thumbnails from the camera. *Id.* This interpretation aligns with the typical operation of communication systems, where devices often enter a state of waiting or listening for incoming data or signals. *Id.* In the described scenario, the mobile phone activates and remains in a listening state until it receives the data necessary to display thumbnails from the digital camera. *Id.* This waiting period serves as a mechanism for the mobile phone to remain responsive to event notifications and effectively manage the data transmission process between itself and the camera. *Id.* Such listening behaviors are common across various elements in similar patents within the domain, reflecting the standard practices and expectations within the field of communication protocols and device interaction. *Id.*

See also supra [12.5.1] discussion of Bluetooth Sniff Mode. TTI-1030, [195]-[196], [199]-[202].

[12.7]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [12.7]. TTI-1030, [203]-[207]. For example, Hiroishi teaches “[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed.” TTI-1011, Claim 10. A POSITA would have understood

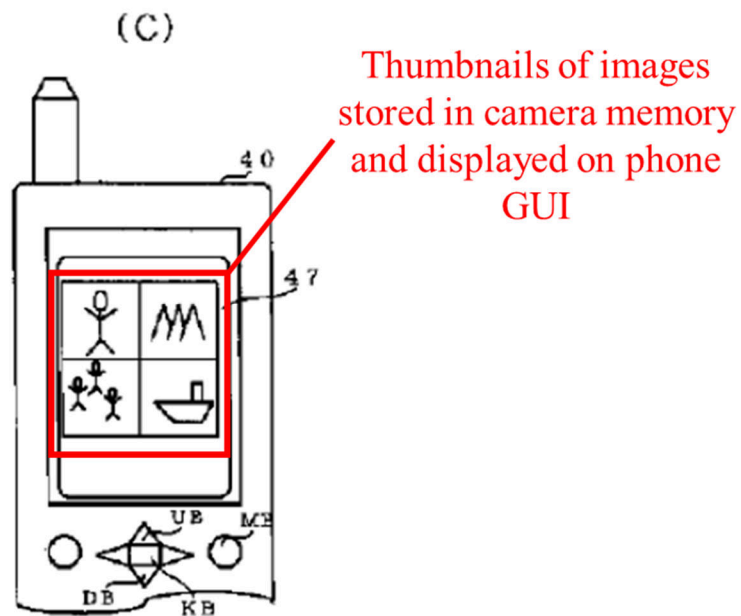
that Hiroishi's program would be alternative term for the mobile software application. TTI-1030, [203]-[207]. The program (mobile software application) is configured to wait for response (listen) for a thumbnail image (an event notification) from the camera over the Bluetooth connection as shown in Fig. 6, the loop until the entire thumbnail is received in step 230, wherein the thumbnail (event notification) is the lower resolution image corresponding to the acquired full resolution image (new-data) and comprises sending a thumbnail over Bluetooth connection from the camera to the phone. *Id.*; TTI-1011, [0081]-[0082], [0104]-[0105]. A POSITA would have understood that the phone's (and/or program installed on the phone (TTI-1011, Claim 10, Abstract) "wait" action for the thumbnail images, constitutes as the phone listening for the event notification signal. *See* Ground 1A, [12.4]; TTI-1030, [203]-[207].



TTI-1011, FIG. 6.

As shown above in FIG. 6, Hiroishi discloses after sending a request to the

digital camera, the cellular phone “waits” for the image data in response. *Id.*, [0102]-[0104]. Subsequently, the camera performs “thumbnail transmission... and the image data for displaying thumbnails is transmitted to the mobile phone 40.” *Id.*, [0102]. While awaiting, the phone receives image data suitable for thumbnail display from the digital camera 50, and subsequently, after decompressing the received image data, it displays the thumbnail on its display unit 47 in Step 232. *Id.*, [0104].



Id., FIG. 7(c) (emphasis added).

The thumbnails correspond to the acquired new data (the image captured by the camera when the release instruction is given). TTI-1030, [203]-[207]. Hiroishi teaches processing digital image data in SDRAM 55A to create thumbnail image data, which is then transmitted to the mobile phone 40 before returning to Step

104. TTI-1011, [0081]-[0082]; *see also id.*, claim 10, [0066]-[0068], [0121].

A POSITA would have also understood that the thumbnails being sent to the phone from the camera constitute the event notification. TTI-1030, [190]-[196], [202]-[207]; *supra* [12.5.1].

[12.8]

The Hiroishi-Takahashi-Bluetooth combination renders obvious step [12.8]. TTI-1030, [208]-[209]. For example, Hiroishi teaches the mobile phone sending a request to the camera for the new data, which are the captured images stored in the camera memory. TTI-1011, [0084], [0105]-[0106]. Hiroishi teaches that the user of the mobile phone can select thumbnail images the user wants to receive from the camera. *Id.* The selection of the images is an instruction sent to the camera for the camera to retrieve the images from memory, process the images, and send the images back to the mobile phone. *Id.*, [0068], [0084], [0105]-[0106]. A POSITA would have recognized that selected image transmission instruction is the request to get new data for transfer. TTI-1030, [208]-[209].

[12.9]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [12.9]. *See* Ground 1A, [12.2]; TTI-1030, [210]-[215]. For example, Hiroishi teaches that the new data (full-resolution images stored in camera memory) are received by the mobile phone in response to the selection of thumbnails. *Id.*; TTI-1011, [0105]-

[0107].

Even though the Bluetooth specification requires encryption support, a POSITA would have found it obvious that encrypting the new data captured by the camera transmitted to the mobile phone offers numerous benefits, primarily ensuring the integrity and security of the data during transfer. TTI-1030, [210]-[215]. Encryption provides a safeguard against potential eavesdropping and unauthorized access, thereby preserving the confidentiality of sensitive information, such as captured images. *Id.*

Furthermore, a POSITA would have had a reasonable expectation of success in implementing encryption for data transmission between the camera and the mobile phone. *Id.* The Bluetooth specification provides comprehensive details and guidelines on how to incorporate encryption mechanisms into communication protocols between Bluetooth-enabled devices. *Id.* With readily available information and resources regarding encryption techniques within the Bluetooth framework, a POSITA would anticipate achieving successful implementation without encountering insurmountable challenges. *Id.*

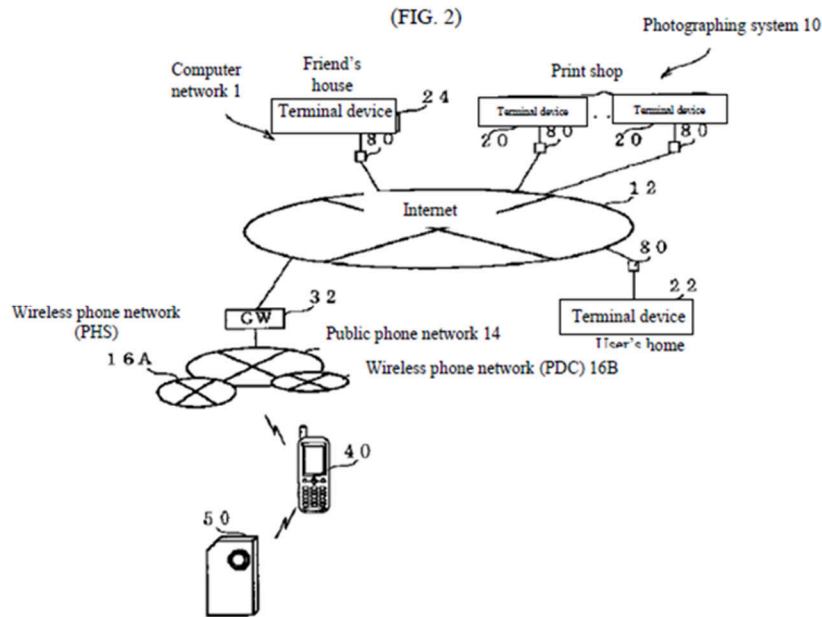
Moreover, it was commonplace within the field for devices to perform encryption on transmitted data to ensure secure communication channels. *Id.* This established practice underscores the familiarity and feasibility of integrating encryption mechanisms into the data transmission process between the camera and

the mobile phone. *Id.* Once data is encrypted for transmission, decryption becomes a necessary counterpart to ensure that the recipient device can access and utilize the transmitted information. *Id.* The Bluetooth specification also offers detailed insights into how to perform decryption, thereby enabling a POSITA to effectively implement the decryption process on the receiving end. *Id.*; TTI-1019, 299.

In summary, given the advantages of encryption, the readily accessible information on encryption techniques in the Bluetooth specification, and the common practice of securing data transmission, it would have been obvious to a POSITA to use encryption to safeguard the integrity and confidentiality of data transferred from the camera to the mobile phone, and to incorporate decryption for accessing the encrypted data on the receiving device. TTI-1030, [210]-[215]; TTI-1019, 299, 1038.

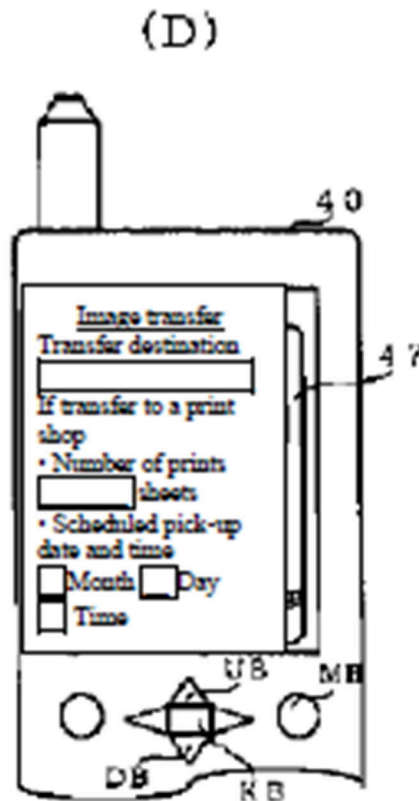
[12.10.1]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [12.10.1]. TTI-1030, [216]-[221]. As discussed above, Hiroishi establishes that the mobile phone can communicate with one or more remote servers using a wireless phone network. Hiroishi teaches configuring the obtained new data with a destination web address. *Id.* In Hiroishi, the email address of the remote terminal is used for uploading the images to the remote terminal. *Id.*; TTI-1011, [0110].



TTI-1011, FIG. 2.

Hiroishi teaches configuring the obtained new data to comprise an action setting to include commands by the user. TTI-1030, [216]-[221]. For example, Patent Owner's infringement contentions identify for this limitation that the "uploaded data includes the command provided by the user such as 'like' or 'scroll down.'" *E.g.*, TTI-1036, 469. The action setting of Hiroishi includes user instructions for a number of sheets for printing and a schedule pick-up date and time. TTI-1030, [216]-[221]; TTI-1011, FIG. 7D.



TTI-1011, FIG. 7D

Hiroishi is silent as to the action setting comprising a HTTP method.

However, a POSITA would have found it obvious to use HTTP methods for an action setting. TTI-1030, [216]-[221]. Takahashi teaches transmitting images to a remote server using HTTP. TTI-1014, [0068]-[0072]. Takahashi teaches a system that allows a mobile device to use HTTP to upload image data to a remote server. TTI-1014, [0037], [0052], [0062], [0068]-[0072], Abstract, Fig. 2. The user can choose what images to publish and share. *Id.*, [0063].

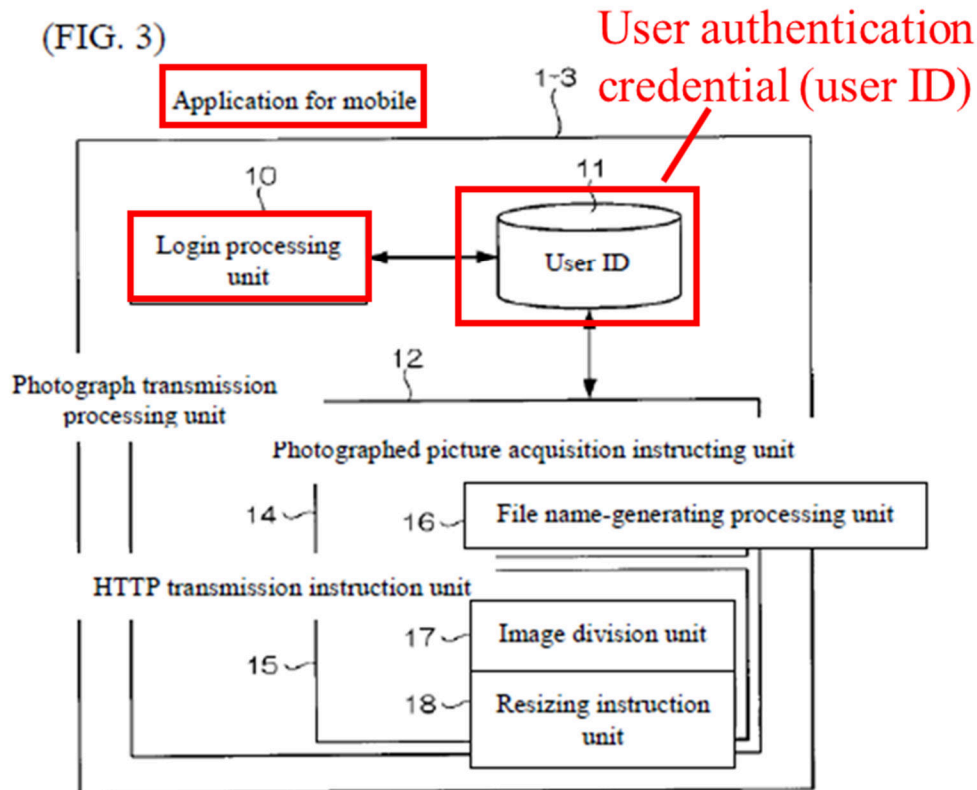
Given the widespread use of HTTP, a POSITA would have understood that

Hiroishi's mobile phone would have implemented communication with network 12 using HTTP. TTI-1030, [216]-[221]. Specifically, it would have been obvious for Hiroishi's phone application to use HTTP (as taught by Takahashi) to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data network). *Id.*

[12.10.2]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [12.10.2]. TTI-1030, [222]-[225]. A POSITA would have found it obvious to also include an email address or other identification information for the operator of the mobile phone with the images sent to the remote server, such as the print shop, so that images could be associated with the operator. *Id.* Even though Hiroishi discusses using caller ID to authenticate the operator when collecting the printouts, a POSITA would have recognized that the photographic system would have benefited from some identifying information associated with the images when they are transferred to the remote server. *Id.* Otherwise, how would the print shop know which images belong to which operator? After the images are identified as being for the operator, the operator can then be authenticated using the caller ID. *Id.*

For example, in the same field of endeavor, Takahashi discloses a “mobile terminal with a login processing means for logging-in to the server.” TTI-1014, [0010]; TTI-1030, [222]-[225].



TTI-1014, FIG. 3 (annotated).

After the initial configuration of the user account, Takahashi clearly discloses that login processing unit would have stored user ID locally within the memory of the mobile phone. *Id.*, [0055]. This stored device identifier enables the user to access the online service provider in subsequent interactions with the remote server. *Id.*; TTI-1030, [222]-[225].

On the remote server end, “[t]he login process unit 21 performs authentication concerning login into the web page published. In particular, in this embodiment, pre-registered users are permitted to access the image storage server 4 for storing image data.” TTI-1014, [0060].

[15.P]

See Ground 1A, [12.P].

[15.1]

See Ground 1A, [12.1].

[15.2]

See Ground 1A, [12.2].

[15.3]

See Ground 1A, [12.4].

[15.4]

See Ground 1A, [12.5].

[15.5]

See Ground 1A, [12.6].

[15.6]

See Ground 1A, [12.7].

[15.7]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [15.7]. TTI-1030, [233]. For example, Takahashi discloses that the new data picture is

saved in a file along with a first timestamp of the time the picture was taken. TTI-1014, [0070], (“The captured photograph is acquired...a file name is generated using the user ID...and the time and date”).

[15.8]

See Ground 1A, [12.9].

[15.9]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [15.9]. TTI-1030, [235]. For example, Takahashi discloses that the new data picture is saved in a file (new data object) along with a first timestamp of the time the picture was taken. TTI-1014, [0070]. Secondly, Takahashi discloses adding another (second) timestamp when a new data picture is selected from among a plurality of pictures to be transmitted to the image server 4. *Id.*, [0087]. Thirdly, Takahashi discloses that when the new data picture is published, an email (that a POSITA would understand to contain a third timestamp) is sent (“ image storage server 4 generates the URL of the web page on which the image selected on the mobile phone side is published (Sf8), and the e-mail containing the generated URL is transmitted to the selected destination”). *Id.*, [0077]. As described, in the Hiroishi-Takahashi-Bluetooth system, the new data picture received by the mobile device is encrypted. *See* Ground 1A, [12.9]; TTI-1030, [235].

[15.10]

See Ground 1A, [12.10], [15.9].

[1.P]

See Ground 1A, [12.P].

[1.1]

See Ground 1A, [12.1].

[1.2]

See Ground 1A, [12.2].

[1.3]

See Ground 1A, [12.3].

[1.4]

See Ground 1A, [12.4].

[1.5]

See Ground 1A, [12.5].

[1.6]

See Ground 1A, [12.6].

[1.7]

See Ground 1A, [12.7].

[1.8]

See Ground 1A, [12.6].

[1.9]

See Ground 1A, [12.7].

[1.10]

See Ground 1A, [12.7].

[1.11]

See Ground 1A, [12.9].

[1.12]

See Ground 1A, [12.10.1]-[12.10.2].

[6.P]

See Ground 1A, [1.P].

[6.1]

See Ground 1A, [1.1].

[6.2]

See Ground 1A, [1.2].

[6.3]

See Ground 1A, [1.4].

[6.4]

See Ground 1A, [1.5].

[6.5]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [6.5]. *See* Ground 1A, [12.6]; TTI-1030, [255]. As discussed above (*see* Ground 1A [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone “waits” to receive the thumbnails from the camera. A POSITA

would recognize this thumbnail transmission instruction to the camera as the mobile phone registering for the data signal notifications (the thumbnails). TTI-1030, [255].

[6.6]

See Ground 1A, [1.9].

[6.7]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [6.7]. TTI-1030, [257]. For example, Takahashi discloses that the new data picture is saved in a file along with a first timestamp of the time the picture was taken. TTI-1014, [0070]; *see also* Ground 1A; [15.9]; TTI-1030, [257].

[6.8]

See Ground 1A, [1.11].

[6.9]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [6.9]. See Ground 1A, [12.10.1]-[12.10.2]; TTI-1030, [216]-[221], [259]-[260].

The “***data signal notification***” is disclosed by Hiroishi as the thumbnails that are “transmitted according to the thumbnail transmission instruction information” to the mobile phone 40. TTI-1030, [259]-[260]; TTI-1011, [0067], [0084]. The mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable the “data signal notification” corresponding to the

new data. The full-resolution images stored in memory are the “new data,” and therefore, the thumbnails are the “data signal notification” of the capture of the new data. TTI-1030, [259]-[260]. Likewise, the thumbnails “correspond” to the new data and serve as a data signal notification because the thumbnails are a lower resolution representation of the full-resolution images stored in memory on the camera. *Id.*

[2]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [2]. TTI-1030, [261]. For example, Hiroishi teaches that the camera includes an internal short-range wireless communications module. *Id.*; TTI-1011, Fig. 4, [0058], [0067].

[7]

See Ground 1A, [2].

[11]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [11]. TTI-1030, [263]. For example, Takahashi discloses that the new data picture is saved in a file along with a first timestamp of the time the picture was taken. TTI-1014, [0070], (“The captured photograph is acquired...a file name is generated using the user ID...and the time and date”); *see also* Ground 1A; [15.9]. A POSITA would understand that Takahashi’s time and date is a timestamp in absolute time. TTI-

1030, [263].

[13]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [13]. TTI-1030, [264]. For example, Hiroishi discloses the new data can be at least image data, and video data but states that the embodiment is not limited to still pictures. *Id.*; TTI-1011, [0068], [0079], [0093], [0123].

[4]

See Ground 1A, [13].

[9]

See Ground 1A, [13].

[14]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [14]. TTI-1030, [267]. For example, Hiroishi discloses that after a user selects a picture transfer from the event notification thumbnail images, the full resolution image is processed by the camera for transfer to the mobile phone. *Id.*; TTI-1011, [0084].

[5]

See Ground 1A, [14].

[10]

See Ground 1A, [14].

[16]

See Ground 1A, [13].

[17]

See Ground 1A, [14].

[18]

The Hiroishi-Takahashi-Bluetooth combination renders obvious [18]. *See* Ground 1A, [11]; TTI-1030, [272]. Takahashi teaches that the time is added based on an internal clock, which could indicate relative time or absolute time. *Id.*; TTI-1012, [0070].

B. GROUND 1B—Claims 1-2, 4-7, 9-18 are obvious over Hiroishi, Kahn, and Bluetooth

1. Kahn

Kahn teaches an imaging system that includes a camera coupled to a cellular phone by a wireless connection. *See, e.g.*, TTI-1017, [0055], FIG. 3. Kahn teaches that the “camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A).” *Id.* The cellular phone can be a “host device” for the camera. *Id.* The cellular phone includes a global positioning module 325. The cellular phone determines a location ID, which is GPS derived longitude and latitude, and sends the location ID with the images to the image server. *Id.*, [0058]. The server can use “the location information may be used to offer location-dependent promotions to the user.” *Id.*, [0051].

In addition, Kahn teaches that the host device (i.e., the cellular phone) “communicates with an online Web-based image management server 330” using,

for example, “HTTP protocol.” *Id.*, [0056].

2. Hiroishi-Kahn-Bluetooth Combination

In the proposed combination, as described by Hiroishi, a photograph system includes a cellular phone that connects to a camera via a Bluetooth connection. TTI-1011, [0066], FIG. 1; TTI-1030, [273]-[274]. The cellular phone controls the camera to capture images, store images, and transmits images to the cellular phone. TTI-1011, [0048], [0049]. The cellular phone then transmits images to a remote computer destination by a cellular network connection via the Internet. *Id.* In the combination, the mobile phone is configured to upload images to a remote terminal or server using HTTP, in a manner similar to what was suggested by Kahn. TTI-1011, [0049]; TTI-1017, [0056]. Also in the combination, the mobile phone sends a user preference that includes global positioning information as taught by Kahn. TTI-1017, [0057]-[0060]. And the mobile application displays an advertisement as taught by Kahn. *Id.*, [0051], [0087]; TTI-1030, [273]-[274].

Also in the combination, the remote terminal includes an authentication server to authenticate the user accessing the remote terminal, as taught by Kahn. TTI-1030, [273]-[274]. The remote terminal also includes a database and a mobile software application advertising software module, as taught by Kahn. *Id.*; TTI-1017, [0062]-[0064], FIG. 4.

3. The Predictable Combination of Hiroishi, Kahn, and Bluetooth

A POSITA at the time of the invention would have been motivated to combine the teachings of Hiroishi (which discloses Bluetooth) and Kahn, thus rendering the subject matter of the '030 patent challenged claims (claims 1-2, 4-7, 9-18) obvious. TTI-1030, [275]-[293].

First, both Hiroishi and Kahn are analogous art to the claimed invention, operating in the same field of endeavor: wireless image transfer from one electronic device to another. *Id.* Hiroishi teaches techniques for enabling a mobile device to control a digital camera and transfer image files between and instructions between the two devices. *See, e.g.*, TTI-1011, Abstract, [0066]. Kahn is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an HTTP action setting. *See, e.g.*, TTI-1017, [0056], [0077] (describing the action setting of creating a new album on the server for uploading the images).

Hiroishi and Kahn are also pertinent to the problem of the '030 patent: transmission of image data by a cellular phone that was captured by a digital camera. TTI-1001, Background; TTI-1030, [275]-[293]. Hiroishi addresses this problem through Bluetooth wireless data transmission and software-based control of the digital camera from the mobile device. *See, e.g.*, TTI-1011, [0043], [0053],

[0061]. Kahn addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g.*, TTI-1017, [0056], [0063].

Second, a POSITA would have been motivated to use Kahn's upload technique to publish image data received at the mobile device of Hiroishi. TTI-1030, [275]-[293]. At the time of the alleged Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g., id.*; TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server); TTI-1018, 5:25-28; TTI-1022, [0032].

Kahn also teaches a camera wirelessly connected to a mobile phone for capturing images and uploading images to a remote server. *See, e.g.*, TTI-1017, [0045], [0055]; *see also* TTI-1011, [0015], [0047], FIG. 2.

Kahn recognizes both of these trends and teaches an efficient and predictable technique for uploading image data (captured by a camera) from a mobile device to a publishing website. *See, e.g.*, TTI-1017, [0063]; TTI-1030, [275]-[293].

The teachings of Kahn would have provided straightforward benefit to the user of the mobile device in Hiroishi: predictable upload of image files and an action setting using an existing HTTP connection between the mobile device and a remote (publishing) server. TTI-1030, [275]-[293]. Hiroishi already teaches the desire to transfer image data from a digital camera to a mobile device to a terminal

device. *See, e.g.*, TTI-1011, [0044]. Kahn would have furthered this purpose by allowing the user to share image data over the Internet in a straight-forward and well-known way. TTI-1030, [275]-[293].

Third, there would have been a reasonable expectation of success in combining the teachings of Hiroishi and Kahn. TTI-1030, [275]-[293]. The combination would have required simply packaging the image data from the mobile device of Hiroishi in an HTTP message as Kahn teaches and as what well known at the time for packet data transfer over the Internet. *Id.* Both modifications would have been well within the ability of a POSITA. *Id.* It would also have been obvious to modify Hiroishi to send the action setting, such as the number of pages or schedule for pick-up, using HTTP, in a manner similar to that described by Kahn. *Id.* To the extent that the action setting of Hiroishi is insufficient to meet the limitation, it would have been obvious to modify Hiroishi with an action setting, like that of Kahn. *Id.* For example, it would have been obvious to modify Hiroishi to send an action setting with the images using HTTP to create a new album for the images to be viewed at a friend's terminal or the user's terminal. *Id.* Doing so would have allowed the user to record the images remotely using the well-known and efficient Internet transfer protocol of HTTP used by Kahn. *Id.*

Fourth, a POSITA would have been motivated, and found it obvious, to

include user identifier that uniquely identifies a particular user of the Internet service. TTI-1030, [275]-[293]. Hiroishi already teaches that the email address of the destination terminal is used to send images to the destination terminal. TTI-1011, [0110]. A POSITA would have found it obvious to include the user identifier with the images when transferring the images to the remote internet server. *See, e.g.*, TTI-1017, [0098]. This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., using a database field for user ID. *Id.*, [0098]. In the example scenario of Hiroishi's print shop, the print shop worker can quickly and easily identify the owner of the images by the file name and can validate the owner when providing the printed images. TTI-1030, [275]-[293]. Likewise, the fulfillment center worker of Kahn can easily identify the owner of the images. *Id.*

A POSITA would have also been motivated to combine Hiroishi to include the location ID with the images sent to the remote server, in a manner similar to that taught by Kahn. TTI-1030, [275]-[293]. Hiroishi describes sending the images from the phone to a print shop. *See, e.g.*, TTI-1011, [0049]. In the combination, a POSITA would have recognized the advantage of including location information with the images to identify a print shop (Kahn's fulfillment center) that was close by. *See, e.g.*, TTI-1030, [275]-[293]; TTI-1017, [0094].

A POSITA would have found it obvious to modify Hiroishi to include a

timestamp with the images, in a manner similar to that suggested by Kahn. TTI-1030, [275]-[293]. As taught by Kahn, it was well known at that time (of the Kahn filing) that imaging devices recorded information about the date/time (timestamp) that an image was captured. TTI-1017, [0008]. This timestamp information provided information about when the images were captured. *Id.* In Kahn's system, the "image data already includes timestamp information (i.e., timestamp indicating when the image is captured)." *Id.*, [0060]. Kahn explains that the timestamp information is useful for correlating timestamps with historical location information. *Id.* A POSITA implementing Hiroishi's system would have found it obvious to include the timestamp information, as was well known practice at the time, according to Kahn. *See, e.g.*, TTI-1030, [275]-[293]; TTI-1017, [0008]. The timestamp information is also valuable so that images transmitted to remote servers could be organized by date. *See, e.g.*, TTI-1017, [0098]. A POSITA would have had a reasonable expectation of success implementing a timestamp into the system of Hiroishi because including timestamp information into images recorded by digital cameras was a well known practice at the time. TTI-1030, [275]-[293]; TTI-1017, [0008].

As discussed above (*supra* §VI.A.4 and Ground 1A, [12.9] for combination between Hiroishi and Bluetooth), a POSITA would have recognized the benefits of implementing encryption of data in the Hiroishi-Kahn-Bluetooth combination.

TTI-1030, [275]-[293]. For example, a POSITA would have recognized that encrypting the data protected the data from being intercepted and decrypted by a malicious attacker or other unauthorized accesses. *Id.* A POSITA implementing Bluetooth encryption would have had a reasonable expectation of success encrypting data. *Id.* The Bluetooth Core Specification 2.1 also teaches how to activate encryption between two Bluetooth devices as well as how to perform encryption to protect the payload. TTI-1019, 884, 919, 1038, 1040-1047.

A POSITA would have found it obvious that encrypting the new data captured by the camera before transmission to the mobile phone offers numerous benefits, primarily ensuring the integrity and security of the data during transfer. TTI-1030, [275]-[293]. Encryption provides a safeguard against potential eavesdropping and unauthorized access, thereby preserving the confidentiality of sensitive information, such as captured images. *Id.*

4. Analysis

[12.P]-[12.9]

See Ground 1A, [12.P]-[12.9], TTI-1030, [294]-[332].

[12.10.1]

See Ground 1A, [12.10.1]. Hiroishi-Kahn-Bluetooth renders obvious [12.10.1]. TTI-1030, [333]-[338]. Hiroishi is silent as to the action setting comprising an HTTP method. However, a POSITA would have found it obvious

to use HTTP methods for action settings as taught by Kahn. TTI-1030, [333]-[338]. For example, Kahn is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an HTTP action setting. *See, e.g.*, Kahn, [0056], [0077] (describing the action setting of creating a new album on the server for uploading the images). A POSITA would have been motivated to implement teachings of Kahn in Hiroishi's mobile phone to have communication with network 12 using HTTP. TTI-1030, [333]-[338].

Specifically, it would have been obvious for Hiroishi's phone application to use HTTP to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data network). *Id.*

Additionally, Kahn highlights the importance of user credentials for accessing photos, detailing the transmission of login credentials to the photo site's server for validation. Kahn, [0074], [0082], [0084], FIG. 5C (elements 522, 526). For example, Kahn discloses that "the applet [at the cell phone] retrieves the NAI and password" from the cell phone's memory and transmits the login credentials "to the photo site (Web-based server providing image management)" to determine the validity of the user credentials. Kahn, [0082].

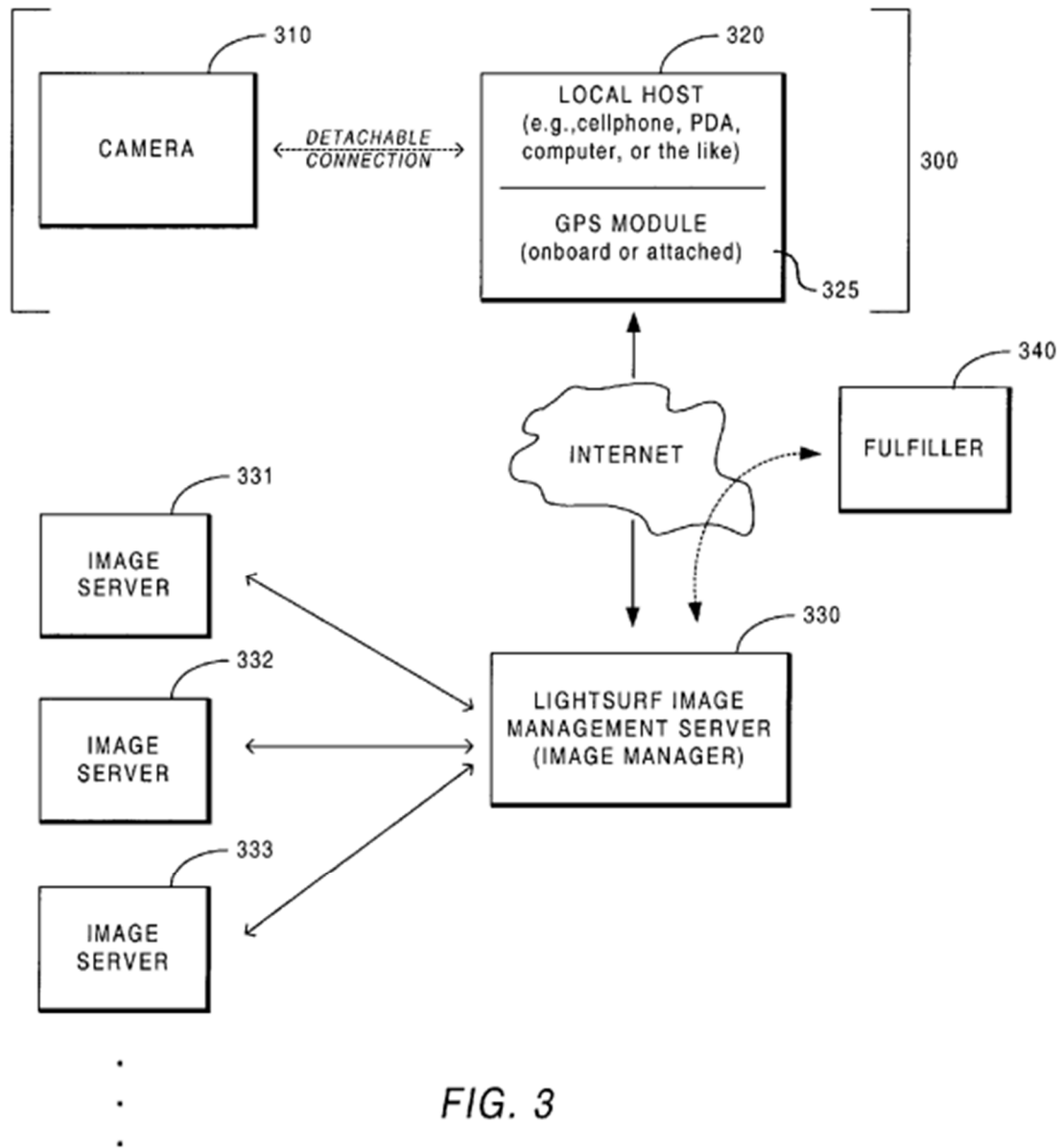


FIG. 3

Id., FIG. 3.

[12.10.2]

Hiroishi-Kahn-Bluetooth renders obvious [12.10.2]. *See* Ground 1A, [12.10.2] (Hiroishi discusses using caller ID to authenticate the operator when collecting the printouts); TTI-1030, [339]-[340]. For example, in the same field of

endeavor, Kahn teaches “transmitting the images from the imaging device to a corresponding user account on a Web server.” TTI-1017, Claim 12, [0057].

[15.P]

See Ground 1B, [12.P].

[15.1]

See Ground 1B, [12.1].

[15.2]

See Ground 1B, [12.2].

[15.3]

See Ground 1B, [12.4].

[15.4]

See Ground 1B, [12.5].

[15.5]

See Ground 1B, [12.6].

[15.6]

See Ground 1B, [12.7].

[15.7]

The Hiroishi-Kahn-Bluetooth combination renders obvious [15.7]. *See* Ground 1B, [12.8]; TTI-1030, [348]. Kahn explains that “prior art imaging devices have...been able to record information about the date/time (timestamp) that an image was captured”. TTI-1017, [0008].

[15.8]

See Ground 1B, [12.9].

[15.9]

The Hiroishi-Kahn-Bluetooth combination renders obvious [15.9]. TTI-1030, [350]. For example, Kahn teaches that “the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)”. TTI-1017, [0050]. As described above (*see* Ground 1B, [12.9]), in the Hiroishi-Kahn-Bluetooth system, the new data picture received by the mobile device is encrypted.

[15.10]

See Ground 1B, [12.10].

[1.P]

See Ground 1B, [12.P].

[1.1]

See Ground 1B, [12.1].

[1.2]

See Ground 1B, [12.2].

[1.3]

See Ground 1B, [12.3].

[1.4.1]

See Ground 1B, [12.4]. Hiroishi-Kahn-Bluetooth teaches acquiring new data

in the Bluetooth enabled data capture device. TTI-1030, [356]-[357].

[1.4.2]

Hiroishi-Kahn-Bluetooth renders [1.4.2] obvious. Hiroishi teaches that the mobile phone 40 and the digital camera 50 are connected by a Bluetooth connection. TTI-1011, [0066]-[0067]; TTI-1030, [358]-[359].

Hiroshi teaches that the camera the digital camera 50 can be operated remotely by the mobile phone 40. TTI-1011, [0043], [0072]. Hiroishi discloses that the digital camera 50 can be instructed to take a photograph through the remote (Bluetooth) connection. *Id.* When the KB key is pressed on the mobile phone 40, it causes the digital camera 50 “to release the shutter” taking a picture and acquiring new data. *Id.*, [0096]. A POSITA would thus understand that because the instructions for remotely taking a picture are received over Bluetooth, the “new data is acquired after the paired secure Bluetooth connection is established”. TTI-1030, [358]-[359].

[1.5]

See Ground 1B, [12.5].

[1.6]

See Ground 1B, [12.6].

[1.7]

See Ground 1B, [12.7].

[1.8]

See Ground 1B, [12.6].

[1.9]

See Ground 1B, [12.7].

[1.10]

See Ground 1B, [12.7].

[1.11]

See Ground 1B, [12.9].

[1.12]

See Ground 1B, [12.10].

[6.P]

See Ground 1B, [1.P].

[6.1]

See Ground 1B, [1.1].

[6.2]

See Ground 1B, [1.2].

[6.3]

See Ground 1B, [1.4].

[6.4]

See Ground 1B, [1.5].

[6.5]

The Hiroishi-Kahn-Bluetooth combination renders obvious [6.5]. *See* Ground 1B, [12.6]. As discussed above (*see* Ground 1B, [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone “waits” to receive the thumbnails from the camera. A POSITA would recognize the thumbnail transmission instruction to the camera as the mobile phone registering for the data signal notifications (the thumbnails). TTI-1030, [373].

[6.6]

See Ground 1B, [1.9].

[6.7]

The Hiroishi-Kahn-Bluetooth combination renders obvious [6.7]. TTI-1030, [375]. For example, Kahn teaches that “the image data already includes timestamp information (i.e., timestamp indicating when the image is captured).” *Id.*; TTI-1017, [0060]; *see also* Ground 1B, [15.9].

[6.8]

See Ground 1B, [1.11].

[6.9]

The Hiroishi-Kahn-Bluetooth combination renders obvious [6.9]. *See* Ground 1B, [1.12]; TTI-1030, [377]-[378]. For example, “the data signal notification” is disclosed by Hiroishi as the thumbnails that are “transmitted according to the thumbnail transmission instruction information” to the mobile

phone 40. TTI-1011, [0067], [0081]-[0084]. The mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable the “data signal notification” corresponding to the new data. TTI-1030, [377]-[378]. The full-resolution images stored in memory are the “new data,” and therefore, the thumbnails are the “data signal notification” of the capture of the new data. *Id.* Likewise, the thumbnails “correspond” to the new data and serve as a data signal notification because the thumbnails are a lower resolution representation of the full-resolution images stored in memory on the camera. *Id.*

[2]

The Hiroishi-Kahn-Bluetooth combination renders obvious [2]. TTI-1030, [379]. For example, Hiroishi teaches that the camera includes an internal short-range wireless communications module. *Id.*; TTI-1011, Fig. 4, [0058], [0067].

[7]

See Ground 1B, [2].

[11]

The Hiroishi-Kahn-Bluetooth combination renders obvious [11]. TTI-1030, [381]. For example, Kahn teaches that it was well known at the time to include a timestamp with image data. *Id.*; TTI-1017, [0008] (describing prior art systems that recorded information about the data/time (timestamp) that an image was captured), [0060]. In Kahn, the timestamp records absolute time for when the

image was recorded. *Id.*

[13]

The Hiroishi-Kahn-Bluetooth combination renders obvious [13]. TTI-1030, [382]. For example, Hiroishi discloses the new data can be at least image data and video data, but states that the embodiment is not limited to still pictures. *Id.*; TTI-1011, [0068], [0079], [0093], [0123].

[4]

See Ground 1B, [13].

[9]

See Ground 1B, [13].

[14]

The Hiroishi-Kahn-Bluetooth combination renders obvious [14]. TTI-1030, [385]. For example, Hiroishi discloses that after a user selects a picture transfer from the event notification thumbnail images, the full resolution image is processed by the camera for transfer to the mobile phone. *Id.*; TTI-1011, [0084].

[5]

See Ground 1B, [14].

[10]

See Ground 1B, [14].

[16]

See Ground 1B, [13].

[17]

See Ground 1B, [14].

[18]

See Ground 1B, [11].

C. Ground 2A—Claims 1-2, 4-7, 9-14 are obvious over Singh129 in view of Bluetooth

Singh129 provides the same disclosure as the '030 patent. *Compare* '030 patent *with* Singh129. Thus, to the extent Patent Owner argues for any limitation that Petitioner did not identify the correct structure in either Singh129, the limitation is nonetheless disclosed in Singh129.

Although Singh129 does not disclose each limitation of the challenged claims (*see* Section V, *supra*), it would have been obvious in view of Bluetooth to modify Singh129's system to: (1) send a message to the Bluetooth enabled mobile device as claimed / receive a message from the Bluetooth enabled data capture device corresponding to a supported data capability of the Bluetooth enabled data capture device; (2) include a timestamp in with the new data object; and (3) encrypt/decrypt the data. TTI-1030, [391]-[392].

A person of ordinary skill in the art would have been motivated to make these modifications to Singh129's data acquisition device and would have reasonably expected to succeed for the same reasons earlier set forth for modifying the Hiroishi/Takahashi and Hiroishi/Kahn combinations. A POSITA would know

how to use Bluetooth for its expected purpose in devices such as those disclosed in Singh129. TTI-1030, [391]-[392]; Ground 1A; Ground 1B.

[12.P]

To the extent the preamble is limiting, the Singh129-Bluetooth combination performs the method recited in [12.P]. TTI-1030, [393]. The Singh129-Bluetooth system performs a method for transferring data (e.g., data acquired by Singh129's digital data capture device 201) to a remote internet server (e.g., Singh129's publishing service 301 and/or website, such as "FlickrTM, PicasaTM, YouTubeTM, eBay®, etc.") by a Bluetooth enabled mobile device (Singh129's mobile device 202). *Id.*; TTI-1009, Abstract, Figs. 1-5 (and related descriptions).

[12.1]

The Singh129-Bluetooth combination performs step [12.1]. TTI-1030, [394]. The Singh129-Bluetooth combination provides a software module (Singh129's client application 203) on the Bluetooth enabled mobile device (Singh129's mobile device 202). *Id.*; TTI-1009, Fig. 2, [0020].

[12.2]

The Singh129-Bluetooth combination performs step [12.2]. TTI-1030, [395]. The Singh129-Bluetooth combination establishes a paired secure connection (a two-way Bluetooth connection) between the Bluetooth enabled mobile device (Singh129's mobile device 202) and a Bluetooth enabled data capture device

(Singh129's digital data capture device 201), wherein the paired secure Bluetooth connection uses cryptographic encryption key(s). *Id.*; TTI-1009, [0021].

[12.3]

The Singh129-Bluetooth combination performs step [12.3]. TTI-1030, [396]-[397]. In the Singh129-Bluetooth combination, Singh129's digital data capture device 201 is modified to send a message corresponding to its supported data capability and the client application 203 on Singh129's Bluetooth enabled mobile device 202 is modified to receive that message. *Id.* Indeed, the Singh129-Bluetooth combination's connection complies with the Bluetooth protocols available in 2007, which described the option to exchange between the Bluetooth devices information regarding supported features. *See* TTI-1019, Section 4.3.4, 441-442. As shown in the cited pages from Bluetooth, the ***max supported page*** is indicative of supported data capability of the Bluetooth enabled mobile device. Other examples of features that are reported include number of slots per packet (3 slot packets or 5 slot packets), Adaptive Frequency Hopping (AFH) capability, Channel Quality Driven Data Rate, and Enhanced Data Rate (EDR). *Id.*, 384-392 (explaining feature definitions); TTI-1030, [396]-[397].

[12.4]

The Singh129-Bluetooth combination performs step [12.4]. TTI-1030, [398]. The Singh129-Bluetooth combination's client application 203 on the

Bluetooth enabled mobile device detects new data (e.g., photographs) acquired by the Bluetooth enabled data capture device (Singh129's digital data capture device 201) for transfer to Singh129's mobile phone 202. *Id.*; TTI-1009, [0023]-[0027].

[12.5]

The Singh129-Bluetooth combination performs step [12.5]. TTI-1030, [399]. In the Singh129-Bluetooth combination, the detecting step (*see* Ground 2A, [12.4]) includes sending a message (*e.g.*, Singh129's polling message and/or the message enabling Singh129's digital data capture device 201 to signal the file event listener of client application 203 in the event a new file is created) to the Bluetooth enabled data capture device 201, over the established paired secure Bluetooth connection, to enable event notifications (the data capture device 201's response to the polling message or its signal to the client application 203 on creation of a new file) on the data capture device 201 corresponding to new data (e.g., photographs), wherein the new data is data acquired by data capture device after establishing the secure Bluetooth pairing connection between the data capture device and the mobile device. *Id.*; TTI-1009, Fig. 1, [0023]-[0027]. A POSITA would have understood that in communications such as Bluetooth, it is advantageous to have the receiver enable transmissions so the receiver is prepared to receive the data. TTI-1030, [399].

[12.6]

The Singh129-Bluetooth combination performs step [12.6]. TTI-1030, [400]. In the Singh129-Bluetooth combination, the detecting step (*see* Ground 2A, [12.4]) includes enabling event notification listening (listening for responses to polling requests and/or using the file event listener in client application 203) on the mobile device 202, to listen for event notifications (“signals”) sent from the data capture device 201, over the established paired secure Bluetooth connection. *Id.*; TTI-1009, [0023]-[0027].

[12.7]

The Singh129-Bluetooth combination performs step [12.7]. TTI-1030, [401]. In the Singh129-Bluetooth combination, the detecting step (*see* Ground 2A, [12.4]) includes receiving, from the Bluetooth enabled data capture device 201, an event notification (the data capture device 201’s response to the polling message or its signal to the client application 203 on creation of a new file) corresponding to existence of new data (e.g., a photograph) for transfer, over the established paired secure Bluetooth connection. *Id.*; TTI-1009, [0023]-[0027].

[12.8]

The Singh129-Bluetooth combination performs step [12.8]. TTI-1030, [402]. In the Singh129-Bluetooth combination, the detecting step (*see* Ground 2A, [12.4]) includes sending a request (e.g., a polling request) to the Bluetooth enabled data capture device 201, to get new data (e.g., a photograph) for transfer to the

mobile device 202. *Id.*; TTI-1009, [0023]-[0027].

[12.9]

The Singh129-Bluetooth combination performs step [12.9]. TTI-1030, [403]. In the Singh129-Bluetooth combination, Singh129's mobile device is modified to encrypt data corresponding to the new data (e.g., a photograph) and send the encrypted data to the mobile device in accordance with the Bluetooth Specification. *Id.* Similarly, Singh129's client application 203 is modified to receive and decrypt the encrypted data using a cryptographic encryption key in accordance with the Bluetooth Specification. *Id.* Accordingly, in the Singh129-Bluetooth combination, the client application of the Bluetooth enabled mobile device 202 is configured to receive the encrypted data over the established Bluetooth paired secure wireless connection and obtain new data (decrypted data) from the received encrypted data using cryptographic encryption key. *Id.*; *see also* Ground 2A, Element [12.2].

[12.10]

The Singh129-Bluetooth combination performs step [12.10]. TTI-1030, [404]. The Singh129-Bluetooth combination's software module (client application) on the Bluetooth enabled mobile device 202 is configured to perform the step of transferring (via email) the obtained new data (e.g., a photograph) along with a user identifier (email address) to a remote internet server (publishing service

401), wherein the transferring step comprises configuring the obtained new data to comprise an action setting (user input) and a destination web address (“websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc.”) of a remote internet server (the email server for the publishing server 401 and/or the servers for the selected websites), wherein the action setting comprises one of a remote procedure call (e.g., “XML-RPC”) method and hypertext transfer protocol (“HTTP”) method, and wherein the user identifier (email address) uniquely identifies a particular user (the user of Singh129’s mobile device 202) of the internet service (publishing) provided by a remote internet server (publishing server 401 and/or the servers for the selected websites). *Id.*; TTI-1009, [0036], [0040], [0047].

[13]

The Singh129-Bluetooth combination performs the method of [13]. TTI-1030, [405]. In the Singh129-Bluetooth combination, the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. *Id.*; TTI-1009, [0009], [0019], [0030], [0043]-[0044], Claim 3.

[14]

The Singh129-Bluetooth combination performs the method of [14]. TTI-1030, [406]. In the Singh129-Bluetooth combination, the event notification corresponds to creation of new data for transfer or change in status of new data for transfer. *Id.*; TTI-1009, [0023]-[0027].

[1.P]

See Ground 2A, Element [12.P].

[1.1]

See Ground 2A, Element [12.1].

[1.2]

See Ground 2A, Element [12.2].

[1.3]

See Ground 2A, Element [12.3].

[1.4.1]

See Ground 2A, Element [12.4]-[12.5.2].

[1.5]

See Ground 2A, Element [12.4]-[12.5.2].

[1.6]

See Ground 2A, Element [12.8].

[1.7]

See Ground 2A, Element [12.5.1].

[1.8]

See Ground 2A, Element [12.5.1] [12.7]. The data capture device would enable event notifications in response to a message to do so.

[1.9]

See Ground 2A, Elements [12.4]-[12.8].

[1.10]

See Ground 2A, Element [12.7].

[1.11]

See Ground 2A, Element [12.9].

[1.12]

See Ground 2A, Element [12.9] (confirming that the Singh129-Bluetooth combination performs the step of transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection and that the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key); Ground 2A, Element [12.10.1]-[12.10.2] (confirming that the mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server); TTI-1030, [419]-[420].

In the Singh129-Bluetooth combination, the mobile device 202 also has

access to the Internet. TTI-1030, [419]-[420]; TTI-1009, Figs. 4-5 (and related descriptions), [0039], [0042], [0044], [0047].

[2]

The Singh129-Bluetooth combination performs the method of claim 2. TTI-1030, [421]. In the Singh129-Bluetooth combination, Bluetooth capability is provided internally in the Bluetooth enabled data capture device in Bluetooth communication device 201a. *Id.*; TTI-1009, Fig. 2, [0020]-[0022], [0031].

[4]

See Ground 2A, Claim [13].

[5]

See Ground 2A, Claim [14].

[6.P]

See Ground 2A, Element [1.P].

[6.1]

See Ground 2A, Element [1.1].

[6.2]

See Ground 2A, Element [1.2].

[6.3]

See Ground 2A, Element [1.4].

[6.4]

See Ground 2A, Element [1.5].

[6.5]

See Ground 2A, Element [12.6].

[6.6]

See Ground 2A, Element [1.9].

[6.7]

See Ground 2A, Elements [15.7]-[15.8].

[6.8]

See Ground 2A, Element [1.11].

[6.9]

See Ground 2A, Element [1.12].

[7]

See Ground 2A, Claim [2].

[9]

See Ground 2A, Claim [13].

[10]

See Ground 2A, Claim [14].

[11]

See Ground 2A, Claim [18].

D. Ground 2B—Claims 15-18 are obvious over Singh129 in view of Bluetooth and Takahashi

It would have been obvious in view of Takahashi to modify Singh129's new data object to include a time stamp corresponding to a time when the new data was

acquired. TTI-1030, [438]. A person of ordinary skill in the art would have been motivated to make this modification and would have reasonably expected to succeed for the same reasons it would have been obvious to add this feature to the Hiroishi/Takahashi and Hiroishi/Kahn combinations. *Id.*; Grounds 1A-1B.

[15.P]

See Ground 2A, Element [12.P].

[15.1]

See Ground 2A, Element [12.1].

[15.2]

See Ground 2A, Element [12.2].

[15.3]

See Ground 2A, Element [12.4].

[15.4]

See Ground 2A, Element [12.5].

[15.5]

See Ground 2A, Element [12.6].

[15.6]

See Ground 2A, Element [12.7].

[15.7]

The Singh129-Takahashi-Bluetooth combination performs step [15.7]. TTI-1030, [446]. As explained in Ground 2A, Element [12.8], in the Singh129-

Bluetooth combination, the step of detecting includes sending a request (e.g., a polling request) to the Bluetooth enabled data capture device, to get new data (e.g., a photograph) for transfer. In the Singh129-Bluetooth combination, the client application also sends a request to get a new data object comprising the new data (e.g., a photograph) and data associated with the new data (“associated files”). TTI-1030, [446]; TTI-1009, [0023]-[0027]. In accordance with Takahashi, the new data object in the combination further includes a timestamp that corresponds to a time when new data was acquired. TTI-1030, [446]; TTI-1014, [0070], (“The captured photograph is acquired...a file name is generated using the user ID...and the time and date”).

[15.8]

See Ground 2A, Element [12.9] (confirming that the client application performs the step of receiving, by the mobile device 202, encrypted new data over the established Bluetooth paired wireless connection). In the Singh129-Takahashi-Bluetooth combination, the data object (*see* Ground 2A, Element [15.7]) is encrypted for the same reason the new data is encrypted in the Singh129-Bluetooth combination. *See* Ground 2A, Element [12.9]. Accordingly, in the Singh129-Takahashi-Bluetooth combination, the client application of the mobile device 202 receives an encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection. TTI-1030, [447]-[448].

[15.9]

See Ground 2A, Element [12.9] (confirming that the client application in the Singh129-Bluetooth combination obtains new data from the received encrypted data object using cryptographic encryption key). In the Singh129-Takahashi-Bluetooth combination, the data associated with new data and the timestamp are obtained from the received encrypted data in the same way. TTI-1030, [449].

[15.10]

See Ground 2A, Element [12.10]; Ground 2B, Element [15.9].

[16]

See Ground 2A, Claim [13].

[17]

See Ground 2A, Claim [14].

[18]

The Singh129-Takahashi-Bluetooth combination performs the method of Claim [18]. TTI-1030, [453]. In the Singh129-Takahashi-Bluetooth combination, the timestamp is added based on an internal clock, which could indicate relative time or absolute time, in accordance with Takahashi. *Id.*; TTI-1014, [0070]; TTI-1030, [453].

VII. DISCRETIONARY CONSIDERATIONS

A. The *Advanced Bionics* Test Favors Institution—§325(d)

Advanced Bionics and the *Becton* factors strongly favor institution.

Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential); *Becton, Dickinson and Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017) (precedential). Under Part I of the two-part framework, the board considers “whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office.” *Advanced Bionics*, IPR2019-01469, Paper 6 at 7-9. Here, substantially the same grounds had not been previously presented to the office.

B. The *Fintiv* Factors Favor Institution—§314(a)

The PTAB considers a set of non-exclusive factors (the *Fintiv* factors) in determining whether to institute an IPR proceeding where there is parallel district court litigation. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). On June 21, 2022, Director Vidal issued “binding agency guidance” entitled “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation.” TTI-1034 (hereinafter the “Interim Guidance”). This Interim Guidance presents “several clarifications... to the PTAB’s... application of *Fintiv* to discretionary institution where there is parallel litigation.” *Id.*, 2.

One clarification provided by the Interim Guidance specifies the effect of

particular types of stipulations presented by petitioners on the Board’s application of the *Fintiv* framework. *Id.*, 3, 7-8. In particular, the Interim Guidance unequivocally states that “***the PTAB will not discretionarily deny institution*** of an IPR or PGR in view of parallel district court litigation where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition.” *Id.*, 7 (emphasis added) (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)). In the present case, Petitioner presents a stipulation, should institution be granted, not to pursue in the parallel district court proceeding the same grounds as in the Petition or any grounds that could have reasonably been raised in the Petition if this IPR is instituted. *See* TTI-1035. Accordingly, based on the Interim Guidance, institution of the Petition ***should not*** be discretionarily denied in view of the parallel district court proceeding. *See* TTI-1034, 7.

VIII. PAYMENT OF FEES – 37 C.F.R. §42.103

Petitioner authorizes the Patent and Trademark Office to charge Deposit Account No. 06-1050.

IX. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

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

TikTok Inc., Bytedance Inc., Bytedance Ltd., Bytedance Pte Ltd., and

TikTok Pte Ltd. are the real parties-in-interest.

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

Petitioner is not aware of any disclaimers, reexamination certificates, or petitions for *inter partes* review for the '030 patent. The '030 patent is the subject of a civil action *CellSpin Soft, Inc. v. ByteDance, Ltd. et al.*, Case No. 2:23-cv-496 (E.D. Tex.).

The '030 patent is in the same family as U.S. Patent Nos. 11,234,121 (“the '121 patent”), 9,900,766 (“the '766 patent”), 8,756,336 (“the '336 patent”), 8,862,757 (“the '757 patent”), 8,898,260 (“the '260 patent”), and 11,659,381 (“the '381 patent”). Petitioner is concurrently petitioning for *Inter Partes* Review of the '121, '766, '336, '757, '260, and '381 patents.

The '030 patent is also in the same family as U.S. Pat. No. 9,258,698, which was the subject of IPR2019-00127, IPR2019-00131, IPR2019-01107, and IPR2019-01108.

U.S. Patent Application No. 18/193,686 is in the same patent family as the '121, '766, '336, '757, '260, and '381 patents and is currently pending before the Patent Office.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR50048-0060IP1@fr.com	Kim H. Leung, Reg. No. 64,399 Steven Katz, Reg. No. 43,706 Rishi Gupta, Reg. No. 64,768 Ryan O'Connor, Reg. No. 60,254 Fish & Richardson P.C. 60 South Sixth Street Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR50048-0060IP1@fr.com

D. Service Information

Please address correspondence/service to the above-listed address.

Petitioner consents to email service at IPR50048-0060IP1@fr.com.

Respectfully submitted,

Dated: April 5, 2024

/W. Karl Renner/
W. Karl Renner, Reg. No. 41,265
Kim H. Leung, Reg. No. 64,399
Steven Katz, Reg. No. 43,706
Rishi Gupta, Reg. No. 64,768
Ryan O'Connor, Reg. No. 60,254
Fish & Richardson P.C.
60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00770)

Attorneys for Petitioners

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,884 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: April 5, 2024

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265

Kim H. Leung, Reg. No. 64,399

Steven Katz, Reg. No. 43,706

Rishi Gupta, Reg. No. 64,768

Ryan O'Connor, Reg. No. 60,254

Fish & Richardson P.C.

60 South Sixth Street

Minneapolis, MN 55402

T: 202-783-5070

F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on April 5, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080
UNITED STATES
(856) 266-5145

/Crena Pacheco/

Crena Pacheco
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
pacheco@fr.com