

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TIKTOK, INC.,

Petitioner,

v.

CELLSPIN SOFT, INC.,

Patent Owner

IPR2024-00767

U.S. Patent No. 11,659,381 B2

IPR2024-00768

U.S. Patent No. 11,234,121 B2

IPR2024-00769

U.S. Patent No. 9,900,766 B2

IPR2024-00770

U.S. Patent No. 8,904,030 B2

Before GREGG I. ANDERSON, CYNTHIA M. HARDMAN,
and MICHAEL A. VALEK, *Administrative Patent Judges*.

DECLARATION OF PAVAN M. GAJENDRAGAD



PAVAN M. GAJENDRAGAD
EXECUTED JANUARY 3, 2025

TABLE OF CONTENTS

I.	EXPERT QUALIFICATIONS AND SCOPE	1
II	INFORMATION CONSIDERED	2
III.	LEGAL FRAMEWORK.....	3
IV.	CLAIM CONSTRUCTION	9
V.	BRIEF SUMMARY OF OPINIONS.....	26
VI.	GENERAL RESPONSE TO EXPERT REPORT	27
A.	General Discussion of Prior Art Bluetooth and Bluetooth Specification	28
VII.	SPECIFIC REBUTTAL TO ALLEGED OBVIOUSNESS COMBINATIONS	38
A.	Validity Analysis of the ‘030 Patent.....	39
1.	Ground 1A – Hiroishi in Combination with Takahashi and Bluetooth V2.1	45
2.	Ground 1B – Hiroishi in Combination with Kahn and Bluetooth 2.1	70
3.	Ground 2A – Singh 129 in View of Bluetooth	82
4.	Ground 2B – Singh 129 in View of Bluetooth and Takahashi	82
B.	Validity Analysis of the ‘766 Patent	94
1.	Ground 1: Singh 129 in View of Singh 906.....	94
2.	Ground 2A: Kahn in View of Bluetooth	98
3.	Ground 2B: Kahn in View of Feinberg and Bluetooth	122
C.	Validity Analysis of the ‘121 Patent	126

1.	Ground 1: Hiroishi in view of Kahn, Endsley, and Bluetooth	126
2..	Ground 2: Singh 129 in View of Singh 906.....	153
D.	Validity Analysis of the ‘381 Patent	157
1.	Ground 1: The Combination of Hiroishi, Kahn and Bluetooth	157
2.	Ground 2: Singh 129 in view of Singh 906	183
VIII.	SUMMARY AND CONCLUSION.....	191

I. EXPERT QUALIFICATIONS AND SCOPE

1. My name is Pavan M. Gajendragad. I have been retained by counsel for the Patent Owner in this matter, Cellspin Soft, Inc. (“Patent Owner” or “Cellspin”), to provide expert testimony, including this Written Rebuttal Report, on the subject of patent validity under 35 U.S.C. §§ 102-103, and 112. More specifically, I have been asked to provide my opinions in rebuttal to those expressed in the Written Report of David Lett, which I understand was prepared and served on behalf of Petitioners in these related matters. My compensation for my work in this matter is not dependent upon the outcome of any aspect of this matter. I am being compensated at my normal hourly rate of \$250 per hour.

2. I am informed and understand that, for purposes of this Written Report, the “Asserted Patents” are the following United States Patents: (i) 9,900,766 (“the ‘766 Patent”); (ii) 11,234,121 (“the ‘121 Patent”); (iii) 11,659,381 (“the ‘381 Patent”); and (iv) 8,904,030 (“the ‘030 Patent”). I am further informed and understand that, for purposes of this Written Report, the “Challenged Claims” are ALL the claims in the “Asserted Patents.” I am further informed and understand that the “Date of Invention” for the Challenged Claims is December 28, 2007.

3. A true and correct copy of my resume is attached as Exhibit A. I received a Bachelor of Science degree in Instrumentation and Electronics

Engineering from Visveswaraiah Technological University in Tumkur, India, and a Master's degree in Telecommunications from the University of Maryland.

4. In my career, I have nineteen years of experience in various aspects of wired and wireless data technology. I have worked as a Senior Data Analyst at Softbank, a Senior Systems Test Engineer at Qualcomm, a Systems Test Engineer at Airvana, a Software System Test Engineer at Ericsson, a Network Administrator and Web Developer at the University of Maryland, a Software Test Engineer at Infosys Technologies, and as a Hardware Engineer at Mistrel.

5. In my career, I have gained extensive experience in many areas relevant to the technologies of the Asserted Patents, including: (i) wireless telecommunications; (ii) OSI - TCP/IP networking protocols; and (iii) wireless networking technologies (including WiFi, Ultra Wide Band, and Bluetooth).

6. All opinions and facts as stated in this Written Report are true and correct to the best of my knowledge, and all opinions expressed herein are my own. If called upon to testify, I could and would testify to the truth of the following.

II. INFORMATION CONSIDERED

7. In preparing this Written Report, and in addition to my own experience, training, education, and recollections, I considered the following documents and things:

8. The Written Report of David Lett, including all appendices thereto.
9. The various references as identified by David Lett in his Report.
10. The various additional websites, sources, and documents as cited throughout this Written Report.
11. The Court's Claim Construction procedures and status as have been explained to me by counsel and as discussed below.
12. The Asserted Patents and their related file histories.

III. LEGAL FRAMEWORK

13. I am not an attorney, but I have been advised concerning the relevant law relating to the subject matter of this Report.

14. I am informed and understand that, for purposes of the Asserted Patents, the so-called "pre-AIA" versions of the patent statutes are applicable. I am informed and understand that such versions are applicable for all patents which have an effective filing date prior to March 16, 2013.

15. I am informed and understand that, for purposes of the Asserted Patents, the "date of invention" and the "effective filing date" is December 28, 2007 (the date of filing of the original Provisional Application for Patent).

16. I am informed and understand that, for purposes of the Asserted Patents, pre-AIA 35 U.S.C. § 102 is the statutory provision concerning patent validity under the "anticipatory" standard. I understand that, pursuant to the

pertinent provisions of pre-AIA 35 U.S.C. § 102, a person shall be entitled to a patent unless:

(i) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent; or

(ii) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States; or

(iii) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months before the filing of the application in the United States; or

(iv) the invention was described in an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent; or

(v) the invention was described in a patent granted on an application for patent by another filed in the United States before the

invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language; or

(vi) before such person's invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it.

17. I am informed and understand that a claim is invalid as anticipated under 35 U.S.C. § 102 if the “four corners” of a single prior art document describe every element of the claimed invention, either expressly or inherently, such that a Person of Ordinary Skill in the Art (“POSITA”) could practice the invention without undue experimentation. Thus, the prior art reference must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements arranged as in the claim. Based on my reading of David Lett’s Written Report, there is no allegation that any Challenged Claim is allegedly anticipated by any single reference under 35 U.S.C. § 102. As to this point, I agree that no single reference discloses each and every element of any claim of any Asserted Patent.

18. I am informed and understand that pre-AIA 35 U.S.C. § 103 is the statutory provision concerning patent validity under the “obviousness” standard. I understand that, pursuant to the pertinent provisions of pre-AIA 35 U.S.C. § 103, a patent may not be obtained though the invention is not identically disclosed or described as set forth in 35 U.S.C. § 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. I further understand that “obviousness” is a question of law based on underlying factual findings, as follows: (i) the scope and content of the prior art; (ii) the differences between the claims and the prior art; (iii) the level of ordinary skill in the art; and (iv) objective considerations of non-obviousness.

20. Still further, I understand that in order to establish that a given claim is obvious, a party is required to demonstrate that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and further that the skilled artisan would have had a reasonable expectation of success in doing so. Moreover, even beyond the analysis requiring evidence of motivation to combine, it is my understanding that obviousness also

requires some teaching of how the references could in fact be combined to work together.

21. I am further advised and understand that the motivation to combine references requires a preliminary identification of the specific problem being addressed. Such a recital of the problem must not be based on “hindsight reasoning” and must not define the problem in terms of its solution. The problem being addressed is properly characterized as the general problem being confronted by the inventor before the invention was made.

22. I am further advised and understand that references may be combined only when there is an established design need or market pressure to solve a problem, and there are a finite number of identified, predictable solutions, and which are easily traversed. Similarly, a combination is only obvious to try when the art reduces the field to a particular direction and provides indicators as to which parameters are critical.

23. I am further advised and understand that when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be non-obvious.

24. I am further advised and understand that one cannot simply rely on a mere “common sense” obviousness argument; rather, one must support each argument by evidence and reasoned explanation.

25. I am further advised and understand that a prior art reference must satisfy the combined functions of a claimed element. By way of example, I am informed and understand that a software application claimed to perform multiple functions must be likewise present in the prior art in the form of a single application performing the same recited functions (as opposed to two separate applications, each independently performing only certain of the claimed functions).

26. I understand that the burden of establishing the status of a reference as “prior art” lies with the party offering the art as part of its invalidity argument. I am informed and understand that the party offering the alleged prior art must establish that such reference(s) meet the criteria set forth in either 35 U.S.C. §§ 102 or 103. For example, the party offering the art must establish that a given reference qualifies as a “printed publication” or that the invention was “in public use.” Still further, I understand that prior art must be analogous to the art disclosed in the patents at issue; the identified art must be from the same field of endeavor or must be reasonably pertinent to the particular problem the inventor was trying to solve.

27. I am informed and understand that expert testimony is proper with respect to factual issues, such as the state of the pertinent art, how one of ordinary skill in the art would understand the prior art references and the terms of the claims, the level of ordinary skill, whether one of ordinary skill in the art would

have been motivated to combine or modify prior art references in a manner that yields the claimed invention, and whether the prior art teaches away from a claimed invention. On the other hand, I am informed and understand that experts are generally not permitted to offer legal opinions on ultimate issues or provide testimony that is merely a legal conclusion.

28. Additional aspects of the law (as has been provided to me) may be highlighted elsewhere in this Written Report as warranted.

IV. CLAIM CONSTRUCTION

29. I am informed and understand that the District Court in this matter is in the process of carrying out its claim construction role, and both parties have provided specific constructions to many terms in the claims of the Asserted Patents. I am also informed that the parties have exchanged claim construction of key terms as required by the local rules of the district court. In the pending seven IPRs, Petitioner has advanced broad interpretations for all terms of all Asserted Patents, and Petitioner has not requested the construction of any specific term. Below is an example text from the IPR2024-00768 Petition at page 7 (similar text is in all seven Petitions):

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).

30. It is my understanding that Petitioner is seeking to secure narrow constructions of one hundred plus claim terms in the District Court. Exhibit 2002 (Petitioner’s Patent L.R. 4-1, 4-2 and 4-3 Disclosures).

31. I am informed and understand that on December 20, 2024, the parties filed required disclosures with the District Court concerning claim construction. As I understand, below are the five key claim terms that are at issue for the ‘766, ‘121, ‘381, and ‘030 Patents (see Joint Claim Construction and Prehearing Statement, Exhibit 2005):

Terms	[Partial] Agreed Constructions
“Bluetooth enabled data capture device”	“separate and apart from the mobile device and has the ability to send and/or receive Bluetooth wireless messages”
“short-range wireless enabled data capture device”	“separate and apart from the short-range wireless enabled cellular phone and has the ability to send and receive short-range wireless messages”
“paired”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase)”

“after the paired secure Bluetooth connection is established” / “after establishing a paired Bluetooth connection” “after establishing the short-range paired wireless connection” / “after the short-range paired wireless connection is established”	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device” / “after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone” “after the paired connection is established and maintained on a continuous basis between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
“short-range paired wireless connection”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase) between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
“cryptographically authenticating”	“verified as legitimate by use of encryption and decryption involving an algorithm”
“data signal notification(s)”	“an indication of the presence of newly acquired data”
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)
“user authentication credential”	“data used to verify the identity of the user”

32. I have been asked to discuss these key terms, and to discuss how they would have been understood by a person of ordinary skill in the art, which I do below,

33. It is my understanding that an earlier ‘127 IPR Petition was filed prior to November 13, 2018, and that the Board construed terms of the Challenged Claims using the so-called “broadest reasonable interpretation” in light of the specification (“BRI”).

34. I am further informed and understand that this Board has since adopted a claim construction procedure which follows the principles articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). In essence, I am informed that such procedure seeks to identify how a given claim term would have been understood by a POSITA, in light of the written description and prosecution history. Thus, it is my understanding that earlier decisions based on the “Broadest Reasonable Interpretation” (“BRI”) standard have little to no bearing on the present case, at least insofar as claim construction is concerned.

35. I am informed and understand that, in patent law, there exists a principle that claim terms should be construed consistently for both invalidity and infringement. I am further informed and understand that this principle is well-established, including as discussed in cases such as *01 Communique Lab., Inc. v. Citrix Sys.*, No. 2017-1869, 2018 U.S. App. LEXIS 10614 (Fed. Cir. Apr. 26,

2018). *See also Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003) (“Claim terms must be “construed the same way for both invalidity and infringement”).

36. It is my understanding that the term “after the paired secure Bluetooth connection is established,” as well as similar terms such as “after establishing the short range paired wireless connection” are (or were) disputed in the District Court. I am informed and understand that these terms have been previously construed to mean: “after the paired connection is established and maintained on a continuous basis.” I agree with this construction from the perspective of a person of ordinary skill, and I understand that the parties in the District Court case have stipulated to this construction, as well.

37. The is my understanding that the claim term “along with” is a disputed claim term at the District Court (as it concerns the ’030 Patent), and Cellspin is asking both the courts to construe “along with” as “in addition to.” I agree with this construction.

38. With reference to the ’802 application specification, and specifically at [0047], a POSITA would appreciate that the patentee has clearly stated that “along with” should mean “in addition to.” In my opinion, this evidence is clear:

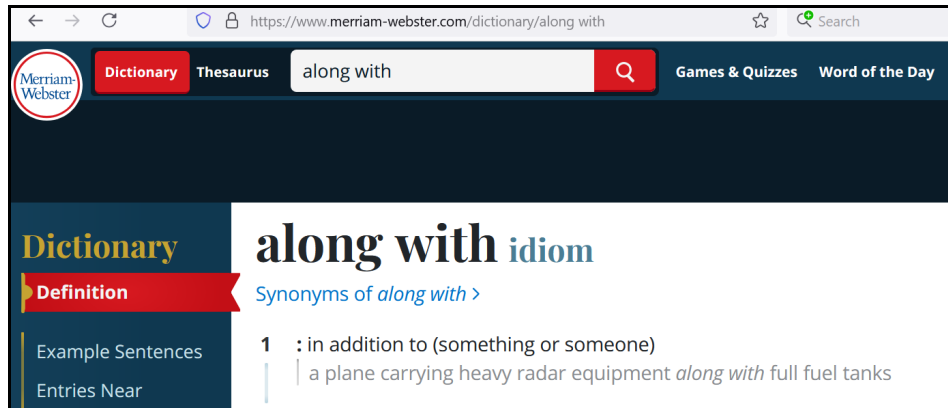
Intrinsic Evidence from the patent specification

[0047] If the user 201 is not satisfied 405 with the created multimedia object, the user 201 may review or delete 406 the multimedia object and start recording again. Otherwise, the user 201 transfers the multimedia object for publishing to a publication space selected by the user 201. Additional information such as the list of the user preferences of the publication virtual spaces 205, authentication identification, user preferences, default settings, manually entered geographical codes, and auction identifiers for eBay® and other shopping websites are selected 407 and transferred along with the user created multimedia content to the publishing service 204. A remote method call 408 such as extensible markup language-remote procedure call (XML-RPC) may be initiated by the client application 202 to transfer the user created multimedia content along with the additional information to the publishing service 204. The transfer to the publishing service 204 takes place using wireless technology, for example, global system for mobile communications, code division multiple access technology, wireless fidelity, or worldwide interoperability for microwave access.

39. Again, the ‘802 specification at [0047] states: “Additional information such as, authentication identification, user preferences, ...and transferred along with the user created multimedia content to the publishing service.” The “client application 202 to transfer the user created multimedia content along with the additional information to the publishing service.”

40. A POSITA would thus appreciate that a variety of information was contemplated as being sent “along with” the multimedia file. Such information included: (i) user preferences; (ii) authentication identification; (iii) user preferences; (iv) default settings; (v) geographical codes; and (vi) auction identifiers. See *id.*

41. I also note that dictionary evidence (*see* <https://www.merriam-webster.com/dictionary/along%20with>) supports this understanding; namely, that “along with” means “in addition to,” as illustrated below:



42. I disagree with the suggestion that the plain and ordinary meaning of “along with” could include “inside.”

43. In my opinion, a POSITA would understand “along with” to mean “in addition to” or “together with,” indicating something is alongside another thing. The concept of “inside,” on the other hand, refers to something being physically contained within the boundaries of another object; essentially, “along with” describes a broader association, whereas “inside” specifies a physical location within something else.

44. In view of the foregoing, it is my opinion that a POSITA would have understood the term “along with” to mean simply “in addition to,” and not including the concept of “inside.”

45. It is my understanding that the term “object” is also disputed by the parties in the District Court case (as relates to the ’030 and ’766 Patents), and that Cellspin proposes the following: “An object can be a variable, a data structure, a function, or a method. Object contains value and is referenced by an identifier.” I agree with this proposed construction.

46. With respect to the “intrinsic record,” it is clear to me that an “object” is different from a “file.” The specification uses multiple terms and does not conflate them. I note that the specification uses the words “object,” “file,” and “data” many times, and further differentiates between “data” and “file” because it describes a “a *data **and** file monitoring* and detection module 203b.”

47. Further, the specification explains: “The digital data capture device 201 then automatically **transfers** 106 the captured **data**, the multimedia content, and the associated files to the client application 203 on the mobile device 202 **using one or a combination of file transfer protocols**. The file transfer protocols may, for example, be one or a combination of BT profile protocols **such as the object exchange (OBEX) protocol**, the generic **object exchange profile (GOEP)** protocol, etc. The file transfer protocols may, for example, also be the media transfer protocol (MTP), the picture transfer protocol **(PTP)**, and the **PictBridge** protocol implemented using a USB.” The specification is very clear that “Data”

can be transferred by using Object based methods like (OBEX and GOEP) or non-object-based methods like MTP and PTP and PictBridge.

48. What the Petition fails to recognize is that, while it is technically possible to send/transfer a “File” using OBEX protocol. *a “File” has to be converted into a “Generic File Object”* for it to be transferred using OBEX. This is illustrated below (Exhibit 2009 (IrDA - OBEX Version 1.3) at 73), wherein “File” is sent as a Generic File Object, but the “File” is not an OBJECT. Rather, it must first be converted into an Object (although the file and file object are different).

9.2 Generic File Object

9.2.1 Introduction

The purpose of this chapter is to outline a method for the exchange of a basic file object [blob] from one device to another. While the OBEX protocol provides many useful headers and capabilities for exchanging objects. This section is designed to provide the reader with an overview of the basic structure used when exchanging generic file data. The file object is assumed to be sent by a generic client to the receiving device's inbox. In a manner consistent to the way QuickBeam and IrXfer applications work. Based on these assumptions, the file exchange should follow the guidelines shown here for headers used and response codes expected.

9.2.2 Commonly Used Headers

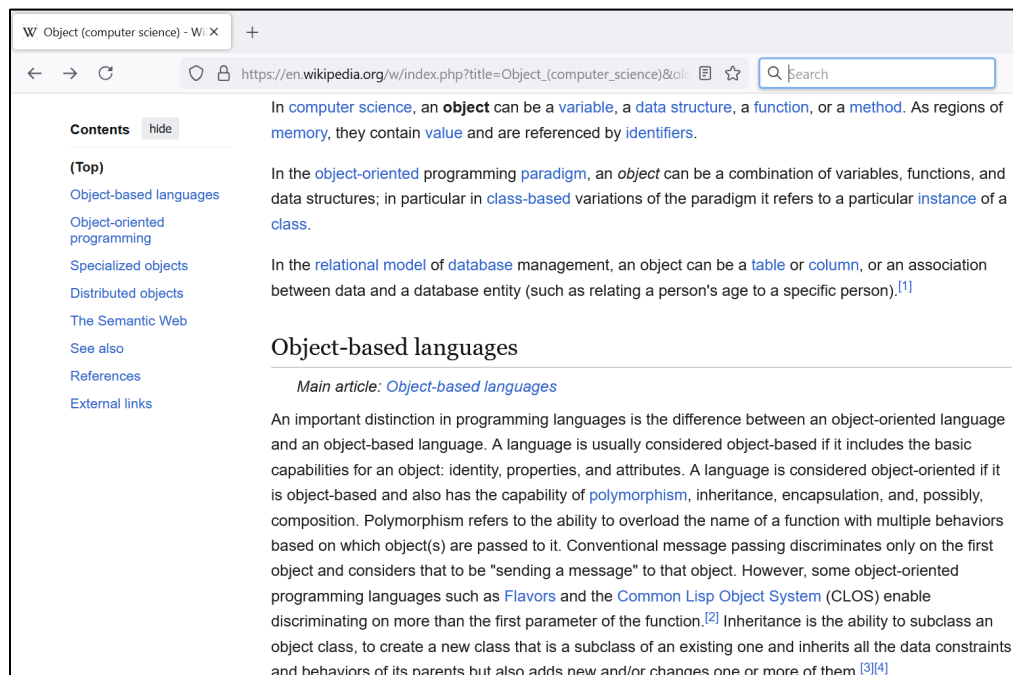
- **Name:** *(Required)* This header is used to convey the full name of the object to exchange. The **Name** header should not contain any path information. If it is necessary to specify a path, it should be done with the **SETPATH** command. All information in this header is interpreted as the objects name.
- **Length:** *(Recommended)* This header is used to convey the size of the file object in bytes. This can be used for verification of storage space requirements. The sum of the bytes passed in **Body** headers should be this many bytes (but is not guaranteed).
- **Body/End-of-Body:** *(Required)* Body headers are used to transfer the file data itself. They are sent repeatedly as long as file data exists to be exchanged. The **End-of-Body** header is used to indicate to the receiving application that this is the last piece of the file data. Applications frequently close the file and consider the transfer complete upon reception of this header. The data contained in the **Body/End-of-Body** headers should be concatenated to form the file.
- **Time:** *(Recommended)* This header is used to exchange the time that the file was last modified. Current file transfer applications use both the simple 4-byte **Time** header and the ISO format. It is recommended that all applications use the more robust ISO **Time** header. For backward compatibility it should be noted that the “IrXfer” application provided by Microsoft only accepts the 4-byte **Time** header. Attempts to send the ISO header will result in the rejection of the operation.
- **Type:** *(Optional)* The MIME type of the file object. This is not often used but can be helpful in some cases to identify the application to associate with the file object.

9.2.3 Response Codes Commonly Used in File Exchange

The following is a list of the known OBEX Response codes that are used during File Object Exchange.

49. Again, and as a POSITA would readily appreciate, a “file” has to be converted to be an “Object” to be sent using OBEX. Similarly, “Data” (that is NOT itself a “File”) can also be converted into an Object and then sent/transferred using OBEX protocol. OBEX is an **object exchange** protocol, **NOT** a file exchange or data exchange protocol, but both file and data can be sent using it by creating an Object first.

50. I further note that Wikipedia confirms the fact that “An **object** can be a variable, a data structure, a function, or a method. Object contains value and is referenced by an identifier.” *See [https://en.wikipedia.org/w/index.php?title=Object_\(computer_science\)&oldid=1111438032](https://en.wikipedia.org/w/index.php?title=Object_(computer_science)&oldid=1111438032):*



51. Still further, the Microsoft Computer Dictionary (Fifth Ed.) (pages 372-373) provides a substantially similar definition of the word “object,” which it

defines as: “a variable comprising both routines and data that is treated as a discrete entity” Object is “that are self-contained collection of data structures.”

object *n.* **1.** Short for object code (machine-readable code). **2.** In object-oriented programming, a variable comprising both routines and data that is treated as a discrete entity. *See also* abstract data type, module (definition 1), object-oriented programming. **3.** In graphics, a distinct entity. For example, a bouncing ball might be an object in a graphics program. **4.** A single, runtime instance of object type that the operating system defines. Objects visible in user mode include event, file, I/O completion port, key, object directory, port, process, section, semaphore, symbolic link, thread, timer, and token objects. Many user-mode objects are implemented through the use of a corresponding kernel-mode object. Kernel-mode-only objects

object-oriented programming *n.* A programming paradigm in which a program is viewed as a collection of discrete objects that are self-contained collections of data structures and routines that interact with other objects. *Acronym:* OOP. *See also* C++, object (definition 2), Objective-C.
Object Pascal *n.* An object-oriented derivative of Pascal. *See also* Pascal.

52. None of these sources suggest that “File” and “Object” are (or can be) the same.

53. Yet still further, the Bluetooth specification itself defines “Object” as: “is composed of Headers which consists of Header ID and Value.”

BLUETOOTH SPECIFICATION Version 1.1page 431 of 1084

IrDA Interoperability Bluetooth™

2 OBEX OBJECT AND PROTOCOL

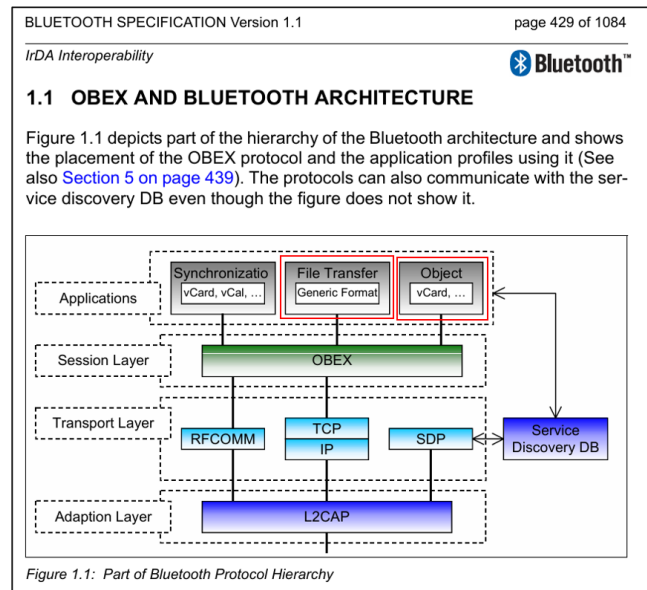
This section is dedicated to the model of OBEX objects and the OBEX session protocol. The section is intended to be read with the IrOBEX specification [1].

2.1 OBJECT

The OBEX object model (Section 2 in [1]) describes how OBEX objects are presented. The OBEX protocol can transfer an object by using the **Put**- and **Get**-operations (See Section 2.2.3 and 2.2.4). One object can be exchanged in one or more **Put**-requests or **Get**-responses.

The model handles both information about the object (e.g. type) and object itself. It is composed of headers, which consist of a header ID and value (See Section 2.1 in [1]). The header ID describes what the header contains and how it is formatted, and the header value consists of one or more bytes in the format and meaning specified by Header ID. The specified headers are **Count**, **Name**, **Type**, **Length**, **Time**, **Description**, **Target**, **HTTP**, **Body**, **End of Body**, **Who**, **Connection ID**, **Application Parameters**, **Authenticate Challenge**, **Authenticate Response**, **Object Class**, and User-Defined Headers. These are explained in detail by Section 2.2 in the IrOBEX specification.

54. A POSITA would understand and appreciate the fact that Object and File are completely different concepts in Bluetooth as well. As shown in OBEX AND BLUETOOTH ARCHITECTURE (2003 Bluetooth Specification, Version 1.1, at page 429), File Transfer and Object Push are **two different** Applications running **on top of OBEX Protocol**.



55. In sum, a POSITA would understand that **Object and File are different**. Thus, a proper construction should account for this fact.

56. It is my understanding that the term “user profile” (as it relates to the ‘381 Patent) is also disputed by the parties in the District Court case, and that Cellspin proposes the following: “a collection of information associated with a user. It contains information such as their Username, Password, Email, Age, Gender, Country/Address.” I agree with this construction.

57. This construction is well-supported by the written description, which recites (at [0006]): “The user creates a user profile on the website of the publishing service.” At [0017] it recites: “The user 201 may also register on the publication virtual spaces 205 by creating a user profile at the publication virtual spaces 205.” At [0021] it recites: “targeted advertisements based on a user profile stored in the database 204a.” At [0025] it recites: “The user 201 may create an account comprising the user profile and login information.” At [0034] it recites: “The database 204a of the publishing service 204 comprises user profiles.” At [0036] it recites: “Targeted advertisements based on the user profile.”

58. I further note that in 2007 a “User Profile” database would have at least these fields, as evidenced by multiple books, articles and MIT papers. *See* computer.howstuffworks.com/internet/social-networking/networks/myspace.htm:

Signing up for MySpace takes about two minutes. To register and create our basic **profile**, all we need to do is enter a few details on a form: name, e-mail address, password, country where we live, postal code (for United States, Canada and United Kingdom residents), gender and birth date. During the initial sign-up, we're also prompted to upload a photo and invite our friends to join.

59. Likewise, *see* “Myspace Maxed Out” Explode Your Popularity, Secure Your Privacy and Buzz Your Band on Facebook (2006) by Bottletree Books. www.google.com/books/edition/Myspace_Maxed_Out/EPbSr4WZ-

nkC?hl=en&gbpv=1&dq=myspace+profile+example&pg=PA71&printsec=frontc

over

MySPACE MAXED ☺ UT -21 -			
Info Type	Info	Info Disclosed by MySpace	To Whom
Sign-Up	Email, First and Last Name, Password, Country, Postal Code, Gender, Birthdate, Age	Email, First Name, Gender, Age	MySpace Community
Profile	Photos, Personal Interests, Gender, Age, Education and Occupation	Photos, Personal Interests, Gender, Age, Education and Occupation	MySpace Community
Non-Personally Identifiable Info	IP Address, Profile Information, Aggregate User Data, and Browser Type	IP Address, Profile Information, Aggregate User Data, and Browser Type	Third Party Vendors to MySpace

60. Still further, *see* “MySpace Unraveled” What it is and how to Use it Safely (2006), by Larry Magid, Anne Collier:

2. Provide your email address, first and last name, date of birth, gender, country, and zip code.

Your email address and last name won't appear in your public profile automatically, but your first name, age, and location will unless you delete them later. (We'll show you how.)

3. Create a unique password with six or more characters, containing at least one number or punctuation character.

4. Agree to comply with basic site-security protocols and the terms of the site by checking the appropriate check box.

5. Enter the characters displayed in the Verification box.

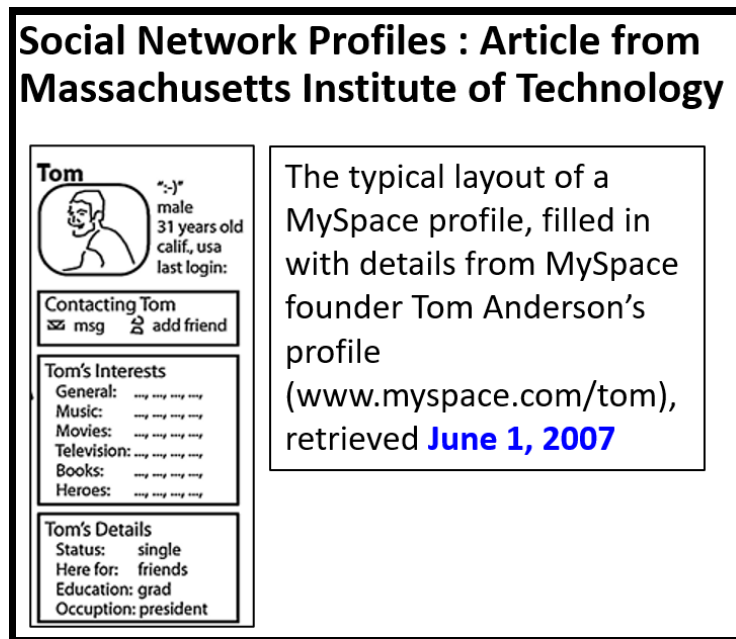
You may have trouble deciphering the verification text, but if you get it wrong, MySpace will display a different one for

61. As of 2007, a POSITA had a good understanding on what “user profile” meant and contained. In 2007, Myspace was valued at \$12 billion and had more than 300 million registered users. *See* <https://en.wikipedia.org/wiki/Myspace>.

62. As a POSITA would have understood, a typical user profile in 2007 required: “a collection of information associated with a user. It contains

information such as their Username, Password, Email, Age, Gender, Country/Address.”

63. This is bolstered by the 2007 article, Social Network Profiles: Massachusetts Institute of Technology (at academic.oup.com/jcmc/article/13/1/252/4583067):



64. Similarly, see https://en.wikipedia.org/wiki/User_profile: “A user profile is a collection of settings and information associated with a user. It contains critical information that is used to identify an individual, such as their name, age, portrait photograph and individual characteristics such as knowledge or expertise.”

65. Still further, the Oracle paper entitled: “How to Build a User Profile” is very clear on what are the most basic attributes of a user profile. See

<https://www.oracle.com/technetwork/topics/ux/applications/user-profile-template-1884996.pdf>

4. What attributes make up a user profile?

While each profile is different, these are some of the key characteristics in an enterprise profile:

- Demographic characteristics – age, gender, location

66. Again, and in view of the foregoing, a POSITA would have understood the term “user profile” in the manner proposed by Cellspin; namely: “a collection of information associated with a user. It contains information such as their Username, Password, Email, Age, Gender, Country/Address.”

67. It is my further understanding that the term “user identifier” is contested by the parties in the District Court case, as it relates to the ‘336, ‘757, ‘030, and ‘260 Patents. It is my understanding that the dispute here concerns a proposal from Petitioner (TikTok) to construe the term to mean “a text string that identifies uniquely a user of a web service and contains sufficient information to authenticate a user of the web service,” to which I understand Cellspin agreed. A POSITA would understand that HTTP (HyperText Transfer Protocol) is an application-layer protocol, based on TEXT. All of the tags, header, etc. are in Text.

Claim Term	Proposed Construction
“user identifier”	“a text string that identifies uniquely a user of a web service”

	Alternatively: “a text string that identifies uniquely a user of a web service and contains sufficient information to authenticate a user of the web service”
--	---

V. BRIEF SUMMARY OF OPINIONS

68. Based on my experience and training, and based on my personal analysis of the various alleged prior art references cited by David Lett and the Challenged Claims, as well as the other documents and things as cited or referenced in this Written Report, it is my opinion that none of the alleged prior art references would have been combined by a POSITA in the manner described by David Lett. Moreover, it is my opinion (in direct contrast to the opinions of David Lett) that the various alleged prior art references and their combinations fail to teach many of the elements of the Challenged Claims, and in certain cases combinations actually lead to “unworkable” solutions, when compared with the inventions as claimed in the Challenged Claims. A POSITA would have had NO reasonable expectation of success in implementing the combinations

69. Based on my experience and training, and based on my personal analysis of the various alleged prior art references cited by David Lett and the Challenged Claims, as well as the other documents and things as cited or referenced in this Written Report, it is my opinion (in direct contrast to the opinions of David Lett) that none of the asserted combinations would have worked

and would lead to unworkable implementation. A POSITA would have had NO reasonable expectation of success in implementing the combinations.

VI. GENERAL RESPONSE TO EXPERT REPORT

70. I have read the entirety of David Lett's Written Report, and I have considered the various documents he cites in support of his positions. My general comments and observations are presented below. Additional details and discussion will follow.

71. David Lett relies upon the same base "combinations" to support his ultimate conclusions that each Challenged Claim is purportedly obvious. I disagree with David Lett. Not only do the specific references (alone or in combination) fail to teach many of the claim limitations, a POSITA would not have been motivated to combine them in the first place. Moreover, and as discussed in greater detail below, there are a number of instances where the alleged prior art actually leads to unworkable solutions and implementation, when compared with the inventions as claimed. A POSITA would have had NO reasonable expectation of success in implementing the combinations.

72. I disagree with David Lett's characterization of the alleged prior art, especially to the extent he erroneously states that the art discloses specific limitations of the Challenged Claims. In the discussion below, I will address each of the references individually, and will point out the many errors in David Lett's

evaluation of the art. Again, in my opinion, the art cited by David Lett fails to teach all limitations of the Challenged Claims, and in any event there would have been no motivation for a POSITA to combine them in the manner relied upon by David Lett.

73. Additional specific rebuttals to David Lett's Written Report follow, below.

A. Discussion of Prior Art Bluetooth and Bluetooth Specification.

74. In my opinion, in order to understand the invention and the Challenged Claims and the prior art it is important to establish an industry standard and definition of certain terms in 2007.

75. A POSITA would have understood "Application Layer" as defined in Microsoft Computer Dictionary Fifth Edition on Page 32, as follows: "The highest layer of standards in Open Systems Interconnection (OSI) reference model. The application layer contains signals that perform useful work for the user, such as file transfer or remote access to a computer, as opposed to lower levels, which control the exchange of data between transmitter and receiver." *See below:*

application layer *n.* The highest layer of standards in the Open Systems Interconnection (OSI) reference model. The application layer contains signals that perform useful work for the user, such as file transfer or remote access to a computer, as opposed to lower levels, which control the exchange of data between transmitter and receiver. See the illustration. *See also* ISO/OSI reference model.

ISO/OSI MODEL	
ISO/OSI Layer	Focus
Application (highest level)	Program-to-program transfer of information
Presentation	Text formatting and display, code conversion
Session	Establishing, maintaining, and coordinating communication
Transport	Accurate delivery, service quality
Network	Transport routes, message handling and transfer
Data-link	Coding, addressing, and transmitting information
Physical	Hardware connections

Application layer. *The highest layer in the ISO/OSI reference model.*

76. Further, it was known and understood that Bluetooth technology maps to the Open Systems Interconnection (OSI) model in the following ways:

Physical layer: The Bluetooth protocol stack's physical layer maps one-to-one to the OSI physical layer. The physical layer is responsible for transmitting and receiving data over the airwaves.

Link layer: The Bluetooth protocol stack's link layer maps to the OSI data link layer. The link layer is responsible for establishing and maintaining a wireless link between devices. It is divided into two sublayers: the Logical

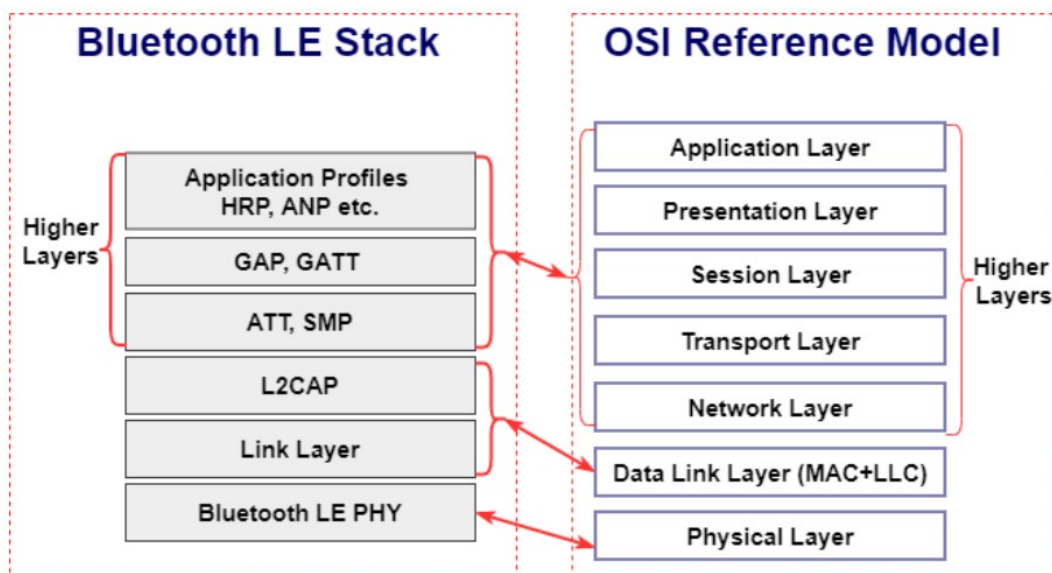
Link Control and Adaptation Protocol (L2CAP) and the Link Manager Protocol (LMP).

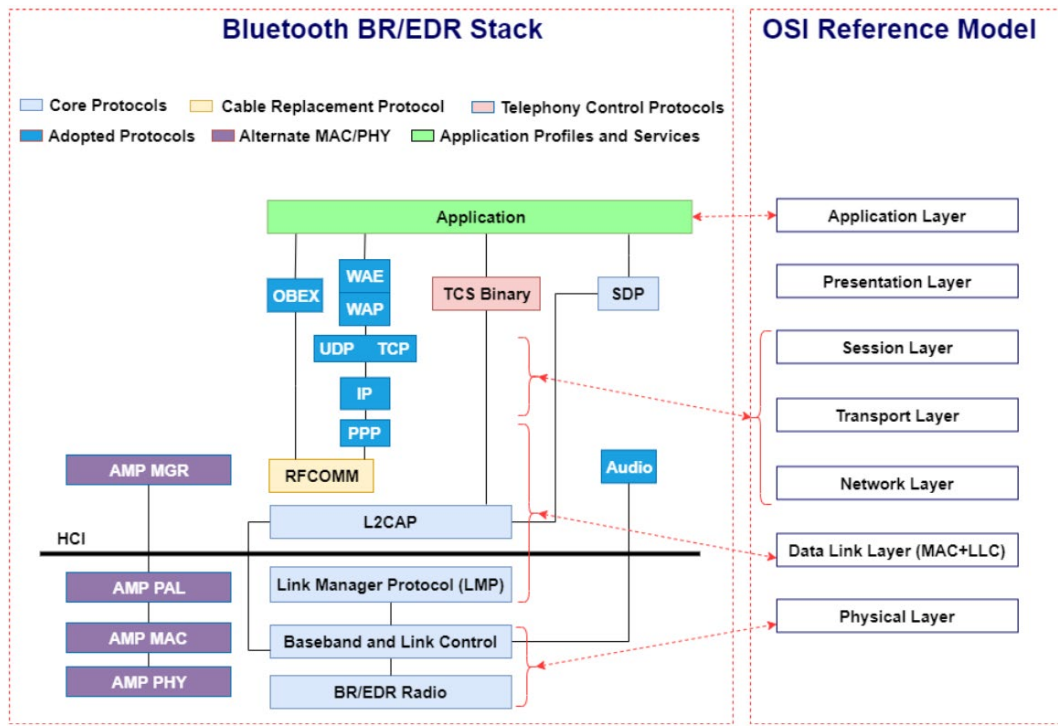
Application layer: Bluetooth profiles, such as SPP (Serial Port Profile), HFP (Hands-Free Profile), and A2DP (Advanced Audio Distribution Profile), operate at the application layer. These profiles define specific use cases and protocols for various applications.

Transport layer: Bluetooth does not directly correspond to the OSI transport layer, but instead relies on L2CAP to provide transport services.

Session layer: Bluetooth does not have a dedicated session layer like the OSI model, but certain Bluetooth profiles define sessions for specific applications.

77. Shown below are the Bluetooth protocol mapping to OSI stack Math works. *See www.mathworks.com/help/bluetooth/ug/bluetooth-protocol-stack.html*





78. In the preceding figure, the Bluetooth protocol stack is shown along with the OSI reference model. There is one-to-one mapping at the physical layer (PHY). The OSI data link layer (DLL) maps to the Bluetooth LE logical link control and adaptation protocol (L2CAP) and link layer (LL). In the Bluetooth stack, the higher layers provide application layer services, device roles and modes, connection management, and security protocol. The functionality of the Bluetooth protocol stack is divided between three main layers: the Controller, the Host, and Application Profiles and Services.

79. As would have been further understood by a POSITA, “Pairing” in Bluetooth is different from “Authentication” and both are different from “Encryption.” As shown in the figure below [Exhibit TTI 1019, p. 19], there are 15

different optional activities after a Bluetooth connection is established, with Pairing, Authentication, and Encryption each being different optional activities. Also, as shown in Figure 3.1 in the v2.1+EDR Bluetooth Core Specification [Exhibit TTI 1019, p. 861] Pairing is different from Authentication and both of them are different from Encryption.

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0]		page 19 of 74
		
2.1	Remote Name Request.....	685
2.2	One-time Inquiry.....	687
2.3	Periodic Inquiry	689
3	ACL Connection Establishment and Detachment.....	691
3.1	Connection Setup	692
4	Optional Activities After ACL Connection Establishment.....	699
4.1	<u>Authentication Requested</u>	699
4.2	<u>Simple Pairing</u> Message Sequence Charts.....	700
4.3	Link Supervision Timeout Changed Event	713
4.4	Set Connection <u>Encryption</u>	714
4.5	Change Connection Link Key.....	715
4.6	Change Connection Link Key with Encryption Pause and Resume.....	715
4.7	<u>Master Link Key</u>	717
4.8	Read Remote Supported Features	719
4.9	Read Remote Extended Features.....	719
4.10	Read Clock Offset.....	720
4.11	Role Switch on an <u>Encrypted Link using Encryption</u> Pause and Resume.....	720
4.12	<u>Refreshing Encryption Keys</u>	721
4.13	Read Remote Version Information	722
4.14	QOS Setup.....	722
4.15	Switch Role	723

All 15 are
Optional

3 ACL CONNECTION ESTABLISHMENT AND DETACHMENT

A flow diagram of the establishment and detachment of a connection between two devices is shown in [Figure 3.1 on page 691](#). The process is illustrated in 9 distinct steps. A number of these steps may be optionally performed, such as authentication and encryption. Some steps are required, such as the Connection Request and Setup Complete steps. The steps in the overview diagram directly relate to the steps in the following message sequence charts.

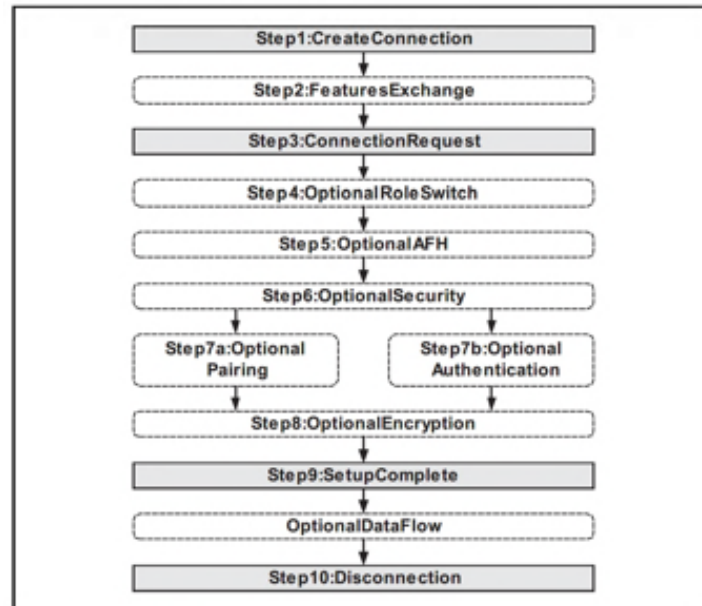


Figure 3.1: Overview diagram for connection setup.

80. For POSITA these options are chosen for a connection depending on the requirements of the solution being implemented. In the Bluetooth family of specifications, Profile specifications are used to describe how to implement a particular use case or family of related use cases. A POSITA would listen to (and comply with) recommendations from the v2.1+EDR Bluetooth Core specification or the Bluetooth Basic Imaging Profile (BIP) specification.

81. With 15 optional activities, there are tens of thousands of combinations of optional activities after ACL connection establishment. Even if all the options are not mutually exclusive, the number of potential and available

combinations is nevertheless extremely large. The Asserted Patents teach one particular combination from this large number of available options. In my opinion it is only through hindsight reasoning that this one particular option is selected by Petitioner, although it clearly was not a simple or obvious design decision in 2007 when the original patent application was filed.

82. Moreover, Petitioner fails to mention the known 2007 pairing disadvantages, such as a poor user experience and battery drain. Even in 2024, there are widely-known “Bluetooth pairing battery issues” that usually refer to a situation where the Bluetooth device, such as headphones or a speaker, rapidly loses battery life when attempting to pair with another device, often due to factors like a weak battery, improper charging, or the Bluetooth connection itself being unstable or not optimized for low power usage.

83. As a POSITA would have understood, maintaining a Bluetooth connection requires power. For example, the Bluetooth radio in your phone consumes energy to stay connected to the earphones, which can lead to faster battery drain. In 2007, a common issue with Bluetooth pairing and battery life was that 2007 Bluetooth technology significantly drained the battery on devices due to its high-power consumption, making it a major concern when pairing devices, especially on portable electronics like phones, as the constant search for connections could quickly deplete the battery.

84. Likewise, known Bluetooth battery issues in 2007 were:

High power usage. Early Bluetooth versions used more power than newer iterations, leading to quicker battery drain when actively searching for or connected to other devices.

Limited battery capacity: Phones and other portable devices in 2007 generally had smaller battery capacities compared to today's standards, making the impact of Bluetooth usage even more noticeable.

Frequent pairing attempts: If you were trying to pair multiple Bluetooth devices or frequently switched between them, it could further exacerbate battery drain due to the continuous search process.

85. The best way to manage Bluetooth battery usage in 2007 was to turn off Bluetooth when not in use: This was the most effective way to conserve battery life as Bluetooth would only drain power when actively searching for or connected to a device.

86. As a POSITA would know, it was these battery issues which led to the development of Bluetooth Low Energy (BLE) because the primary goal of BLE was to significantly reduce power consumption compared to traditional Bluetooth, making it ideal for battery-powered devices like wearables and sensors where long battery life is crucial; essentially, the need to extend battery life in small devices drove the creation of a more power-efficient Bluetooth standard like BLE. As

compared to Classic 2007 Bluetooth 2.1, Bluetooth Low Energy was intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. *See* en.wikipedia.org/wiki/Bluetooth_Low_Energy

87. As of 2007, a POSITA would **NOT** have been inclined to create a system which required pairing devices because the Bluetooth specifications didn't require pairing. Even in 2007 (with Bluetooth 2.1 Security Mode 4) the default security requirement was an unauthenticated link key, which does not require the entry of a PIN, passkey or comparison of a passkey by the user. More specifically, the Bluetooth specification clearly states that: "[w]hen both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption." (Exhibit TTI 1019, p. 1273 and 1286).

88. It would have been these "shall default" Bluetooth options that would have provided for the data security benefits desired by POSITA in 2007. The default connection mode described in the v2.1+EDR Bluetooth core specification is for the connection to be *unpaired, encrypted, unauthenticated and unauthorize*. Exhibit TTI 1019, p. 1273 and 1286. Without some other specific requirement in place for a connection to be paired, there is no reason that a POSITA would not choose the default connection (unencrypted, authenticated and/or authorized).

89. In 2007, a POSITA would NOT choose to "maintain a paired connection on a continuous basis," and Petitioner makes no showing otherwise.

The claim construction the parties have already agreed upon at the District Court is “after the paired connection is established and maintained on a continuous basis.”

90. In 2007 A POSITA would have understood that the Basic Imaging Profile (BIP) describes all the Kahn, Hiroishi, Feinberg, and Endsley scenarios. However, BIP did not require a paired Bluetooth connection for all these scenarios. Rather, for the scenarios most in line with Kahn, Hiroishi, Feinberg, and Endsley (*i.e.* pull based or push based mage transfer), BIP was not recommending using a paired Bluetooth connection.

91. NONE of the cited references (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default *for any scenarios*. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

92. In my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification

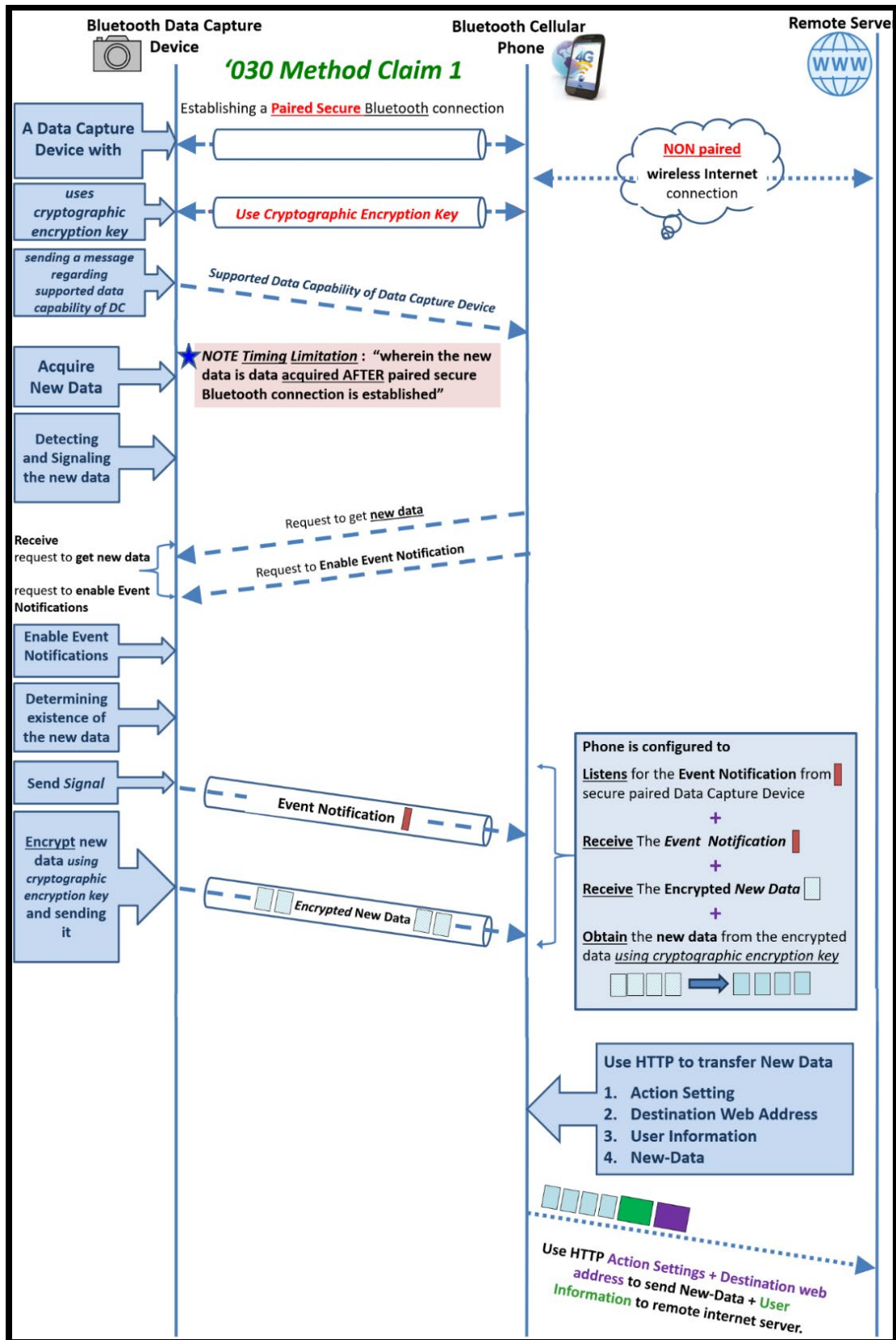
or NOT go with the recommendation provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

VII. SPECIFIC REBUTTAL TO ALLEGED OBVIOUSNESS COMBINATIONS

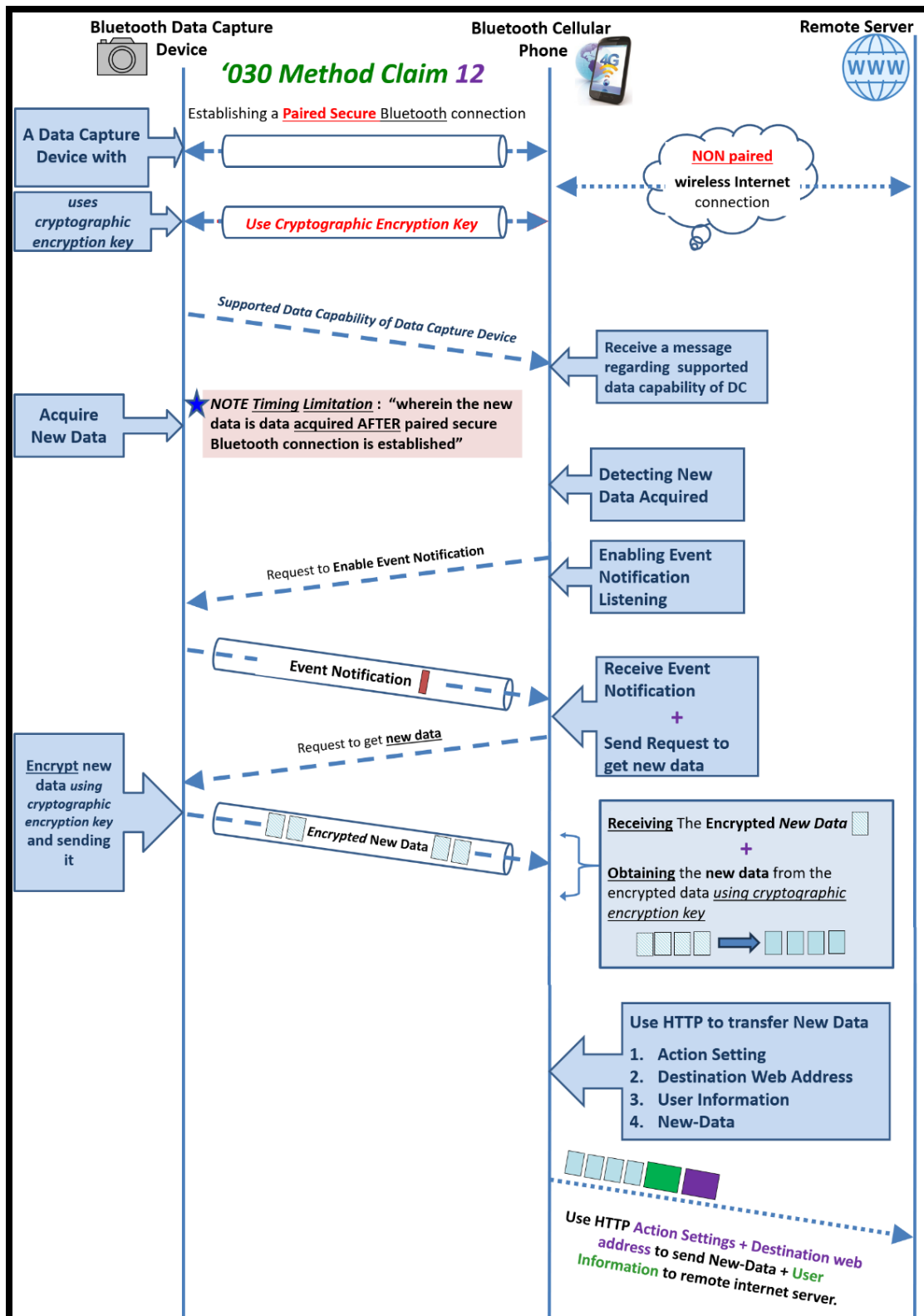
93. As noted above, I do not understand David Lett to have identified any alleged anticipatory references under 35 U.S.C. § 102 in his Report. He has, however, identified a number of combinations which he identifies as purportedly comprising invalidating disclosures under 35 U.S.C. § 103. I disagree with the conclusions drawn by David Lett, and I find that none of the identified art, either alone or in combination, renders any Challenged Claim invalid. My discussion and specific rebuttal of each of the combinations offered by David Lett follows.

A. Validity Analysis of the '030 Patent

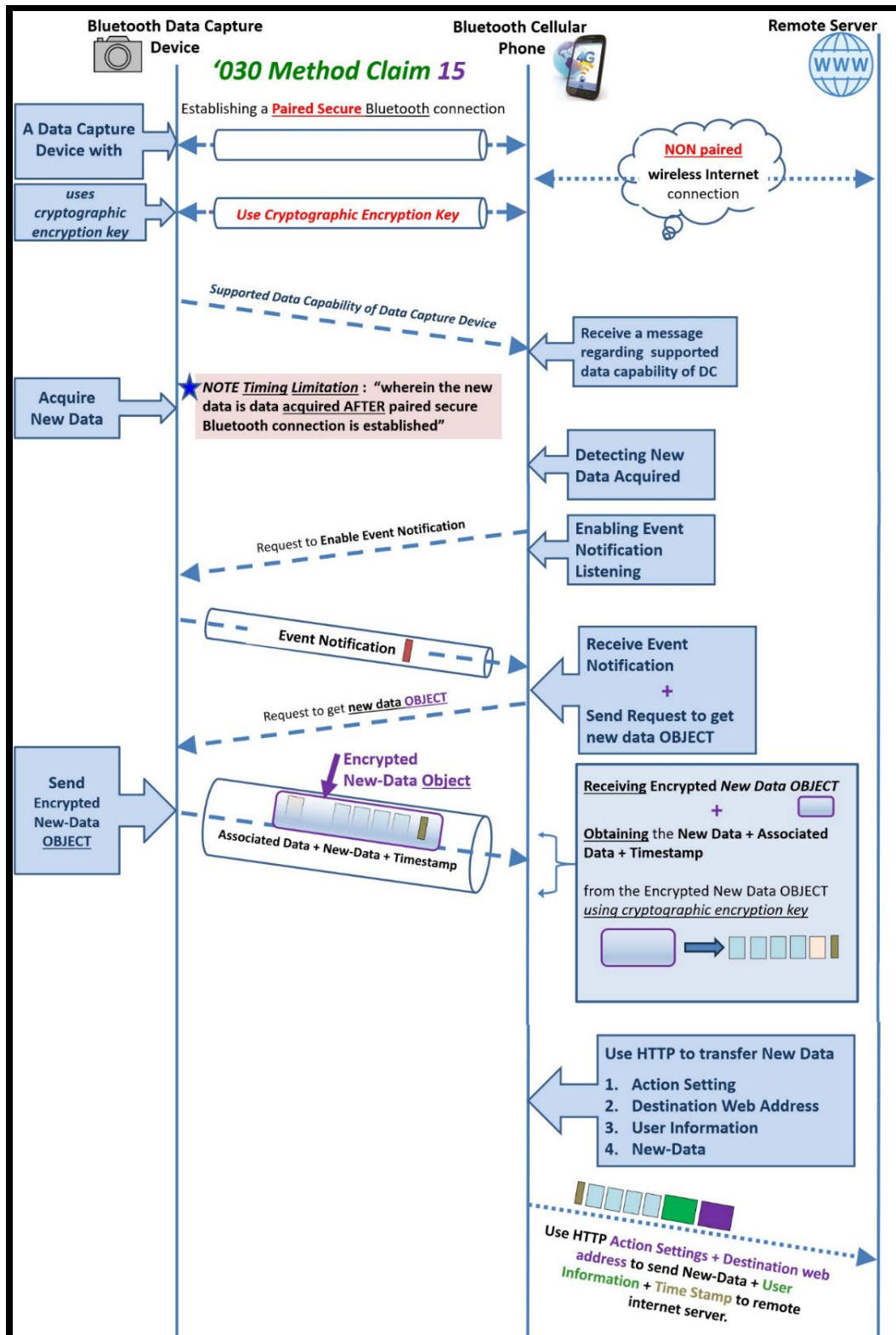
94. As an initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 1 of the '030 Patent as an example):



95. As an additional initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 12 of the '030 Patent as an example):



96. As yet another initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 15 of the '030 Patent as an example):



**1. Ground 1A – Hiroishi in Combination with
Takahashi and Bluetooth v2.1**

97. David Lett suggests that a POSITA would have been motivated to combine the teachings of Hiroishi in Combination with Takahashi and Bluetooth 2.1 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

98. First, as required, and as shown above, I have examined the scope and content of the cited prior art. With respect to teachings of Hiroishi, Takahashi, and Bluetooth v2.1, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Hiroishi in combination with Takahashi and Bluetooth V2.1 reference render the Challenged Claims obvious. I disagree David Lett’s conclusions. Here, I address the most glaring deficiencies in his analysis.

99. The first glaring deficiency in his analysis is that BOTH parties have already agreed and adopted the claim construction for certain key terms, including:

“after the paired secure Bluetooth connection is established” /	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device” /
“after establishing a paired Bluetooth connection”	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone”
“after establishing the short-range paired wireless connection” / “after the short-range	“after the paired connection is established and maintained on a continuous basis between the

paired wireless connection is established”	short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
--	---

100. None of Hiroshi, Takahashi, Kahn or Bluetooth disclose a paired connection that is “established and maintained on a continuous basis,” and Petitioner has not asserted that any cited reference discloses such a connection.

101. NONE of the prior art of record (Kahn, Hiroishi, Takahashi) even mention the word “pair” or “pairing,” let alone any **paired connection which is “established and maintained on a continuous basis.”**

102. **In 2007, a POSITA would definitely NOT “maintain a paired connection on a continuous basis.”** The claim construction the parties have already agreed upon at the District Court is “after the paired connection is established and maintained on a continuous basis.” Once again, I reiterate the fact that NONE of cited prior art discloses a paired connection that is **“established and maintained on a continuous basis.”**

103. The second glaring deficiency in his analysis is that “pairing” is not a “must” for a Bluetooth connection as suggested by the Petitioner, and both Pairing and Cryptographic Authentication are *optional* and not obvious.

104. Petitioner relies solely on the Bluetooth Specification for support for pairing and cryptographically authenticating – not on any disclosure in Hiroshi or Takahashi or even Kahn. BUT, in the Bluetooth standard 2.1, the default for bi-

directional communication with another Bluetooth device is NOT paired and NOT Authenticated; rather, it is just Encrypted.

105. Petitioner argues: “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.”

106. Petitioner further argues: “Bluetooth Core specification describes the process for establishing a secure pairing.” Even though the ‘030 Patent claims do not require cryptographic authentication, Petitioner has included arguments about it in its Petition.

107. I am informed that, in its institution decision (page 42 for ‘121 Patent), the Board stated that “Petitioner, for example, has demonstrated a reasonable likelihood of prevailing in showing that the connection between Hiroishi’s camera and mobile phone *is “paired,” given that there is two-way communication between the devices via Bluetooth.*”

108. As a POSITA would understand and appreciate, it is a fact that two Bluetooth devices can have bi-directional two-way communication between them **without ever pairing** (even today). I thus disagree with the above-referenced statement by Petitioner. In fact, in the Bluetooth standard 2.1, the default for bi-

directional two-way communication with another Bluetooth device is NOT paired and NOT Authenticated. It is just Encrypted.

109. Upon my review, the words “pair,” “paired,” and “cryptographically authenticating” do NOT appear in any cited art, except the Bluetooth Specification. Once again, I reiterate that the Bluetooth standard makes pairing OPTIONAL. This is because it was NOT done before and not recommended for variety of reasons in 2007 and before.

110. It is my understanding that the construction for both “Paired” and “Cryptographically Authenticating” are agreed by the parties in the District Court.

“paired”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase)”
“short-range paired wireless connection”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase) between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
“cryptographically authenticating”	“verified as legitimate by use of encryption and decryption involving an algorithm”

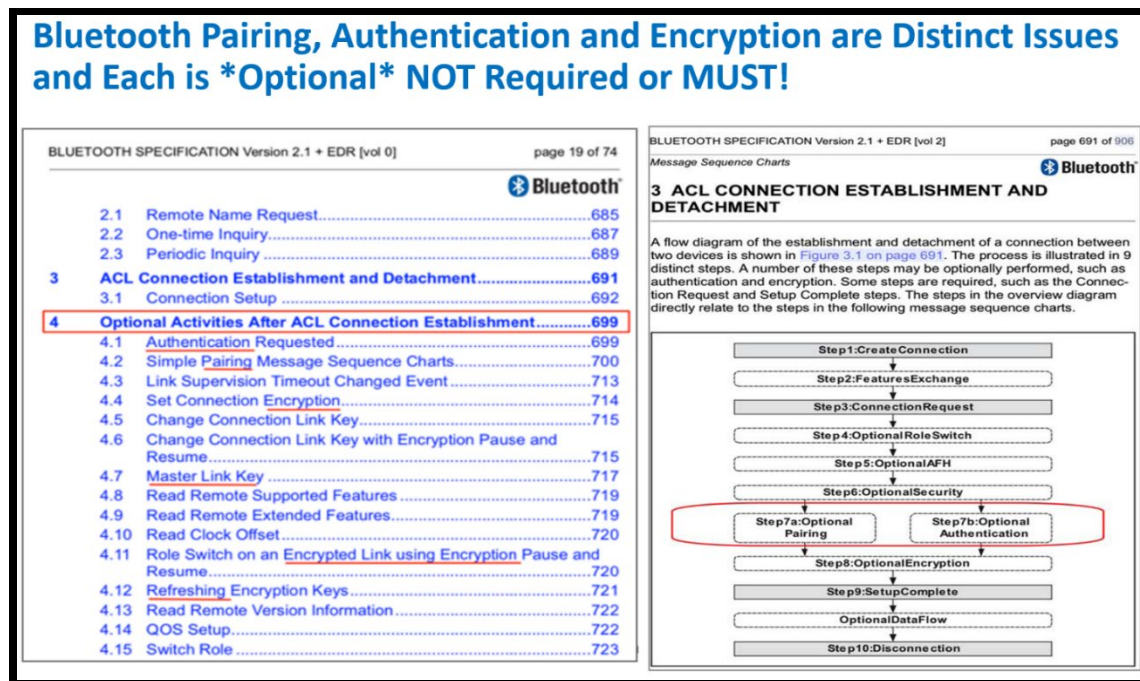
111. Just a mention of Bluetooth in a reference does not mean that it supports pairing or it would be obvious to do so, because several devices in 2007 did not even support pairing in Bluetooth hardware chips. Again, the default 2.1

Bluetooth standard does not require pairing. For example, Bluetooth EDR 2.1 has error codes for when one device attempts to pair with another that does not allow pairing: (1) Pairing Not Allowed (0X18); and (2) Simple Pairing Not Supported (0X37):

Bluetooth Pairing is Optionally Practiced and Optionally Supported	
BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0] page 15 of 74 Bluetooth 5.2 Parameter Definitions 313 5.3 LMP Encapsulated 323 5.4 Default Values 324 6 List of Figures 325 7 List of Tables 329 Part D ERROR CODES Contents 333 1 Overview of Error Codes 335 1.1 Usage Descriptions 335 1.2 HCI Command Errors 335 1.3 List of Error Codes 336 2 Error Code Descriptions 338 2.1 Unknown HCI Command (0X01) 338 2.2 Unknown Connection Identifier (0X02) 338 2.3 Hardware Failure (0X03) 338 2.4 Page Timeout (0X04) 338 2.5 Authentication Failure (0X05) 338 2.6 PIN or key Missing (0X06) 338 2.7 Memory Capacity Exceeded (0X07) 338 2.8 Connection Timeout (0X08) 339 2.9 Connection Limit Exceeded (0X09) 339 2.10 Synchronous Connection Limit to a Device Exceeded (0X0A) 339 2.11 ACL Connection Already Exists (0X0B) 339 2.12 Command Disallowed (0X0C) 339 2.13 Connection Rejected due to Limited Resources (0X0D) 339 2.14 Connection Rejected due to Security Reasons (0X0E) 339 2.15 Connection Rejected due to Unacceptable BD_ADDR (0X0F) 340 2.16 Connection Accept Timeout Exceeded (0X10) 340 2.17 Unsupported Feature or Parameter Value (0X11) 340 2.18 Invalid HCI Command Parameters (0X12) 340 2.19 Remote User Terminated Connection (0X13) 340 2.20 Remote Device Terminated Connection due to Low Resources (0X14) 341 2.21 Remote Device Terminated Connection due to Power Off (0X15) 341 2.22 Connection Terminated by Local Host (0X16) 341 2.23 Repeated Attempts (0X17) 341 2.24 Pairing not Allowed (0X18) 341 2.25 Unknown LMP PDU (0X19) 341 26 July 2007	BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0] page 16 of 74 Bluetooth 2.26 Unsupported Remote Feature / Unsupported LMP Feature (0X1A) 341 2.27 SCO Offset Rejected (0X1B) 341 2.28 SCO Interval Rejected (0X1C) 342 2.29 SCO Air Mode Rejected (0X1D) 342 2.30 Invalid LMP Parameters (0X1E) 342 2.31 Unspecified Error (0X1F) 342 2.32 Unsupported LMP Parameter Value (0X20) 342 2.33 Role Change Not Allowed (0X21) 342 2.34 LMP Response Timeout (0X22) 342 2.35 LMP Error Transaction Collision (0X23) 343 2.36 LMP PDU Not Allowed (0X24) 343 2.37 Encryption Mode Not Acceptable (0X25) 343 2.38 Link Key Can Not be Changed (0X26) 343 2.39 Requested QoS Not Supported (0X27) 343 2.40 Instant Passed (0X28) 343 2.41 Pairing with Unit Key Not Supported (0X29) 343 2.42 Different Transaction Collision (0X2A) 343 2.43 QoS Unacceptable Parameter (0X2C) 343 2.44 QoS Rejected (0X2D) 344 2.45 Channel Classification Not Supported (0X2E) 344 2.46 Insufficient Security (0X2F) 344 2.47 Parameter out of Mandatory Range (0X30) 344 2.48 Role Switch Pending (0X32) 344 2.49 Reserved Slot Violation (0X34) 344 2.50 Role Switch Failed (0X35) 344 2.51 Extended Inquiry Response Too Large (0X36) 344 2.52 Simple Pairing Not Supported By Host (0X37) 345 2.53 Host Busy-Pairing(0X38) 345 Part E HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION Contents 349 1 Introduction 357 1.1 Lower Layers of the Bluetooth Software Stack 357 2 Overview of Host Controller Transport Layer 359 3 Overview of Commands and Events 360 3.1 Generic Events 361 3.2 Device Setup 361 3.3 Controller Flow Control 362 3.4 Controller Information 362 26 July 2007

112. In Bluetooth “Pairing” is different from “Authentication” and both are different from “Encryption. As shown and discussed above, there are 15 different **optional** activities after a Bluetooth connection is established. Pairing, Authentication, and Encryption are different optional activities. Also, as shown in Figure 3.1 in the v2.1+EDR Bluetooth Core Specification [Exhibit TTI 1019, p.

861] it again clearly shows that the Pairing is different from Authentication and both of them are different from Encryption.



113. For a POSITA these options are chosen for a connection depending on the requirements of the solution being implemented. In the Bluetooth family of specifications, Profile specifications are used to describe how to implement a particular use case or family of related use cases. A POSITA would abide by the recommendations from the v2.1+EDR Bluetooth Core specification or the Bluetooth Basic Imaging Profile (BIP) specification.

114. As noted above, there are tens of thousands of possible combinations of optional activities after ACL connection establishment in Bluetooth. Even if all the options are not mutually exclusive, the number of combinations remain a very large number. The Asserted Patents teach one particular combination from the

large number of available options. Again, in my opinion, Petitioner is using hindsight reasoning for something which was not a simple design decision in 2007.

115. Moreover, and as noted and discussed in detail above, Petitioner fails to account for the known pairing disadvantages, such as a **poor user experience and battery drain**.

116. Again, and as noted and discussed above, the best way to manage Bluetooth battery usage in 2007 *was to turn off Bluetooth when not in use*: This was the most effective way to conserve battery life as Bluetooth would only drain power when actively searching for or connected to a device.

117. As noted and discussed in detail above, as of 2007, a POSITA would **NOT** be inclined to create a system which required pairing devices because the **Bluetooth specifications didn't require** pairing. Even in 2007, and for Bluetooth 2.1 Security Mode 4, the **default security requirement was an unauthenticated** link key, which doesn't require the entry of a PIN, passkey or comparison of a passkey by the user.

118. Moreover, Hiroshi [0067] teaches one to follow the Bluetooth Standards: “Therefore, the communication unit 49 of the mobile phone 40 and the communication unit 59 of the digital camera 50 are configured so as to allow a communication according to the standard of Bluetooth, respectively.” For Petitioner to suggest otherwise is contrary to Hiroshi's teaching.

119. Again, and as noted and discussed above, the Bluetooth specification clearly states twice that, “[w]hen both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption.” (Exhibit TTI 1019, p. 1273 and 1286).

120. This statement also means that NOT ALL Bluetooth devices supported pairing. (Conditional statement when both device).

121. As noted and discussed above, it would have been these “shall default” Bluetooth options that would have provided for the data security benefits desired by POSITA in 2007. The default connection mode described in the v2.1+EDR Bluetooth core specification is for the connection to be *unpaired, encrypted, unauthenticated and unauthorize*. Exhibit TTI 1019, p. 1273 and 1286. Without some other specific requirement in place for a connection to be paired, there is no reason that a POSITA would not choose the default connection (unencrypted, authenticated and/or authorized).

122. Even if one were to look at only the security modes described in the 2006 v2.1+EDR Bluetooth Core specification, which is what a POSITA would have consulted for Bluetooth in the 2007 timeframe, there are significantly more options than just paired or unpaired. A more complete list of options is:

- Unpaired, unencrypted, unauthenticated, and unauthorized
- Unpaired, unencrypted, unauthenticated, and authorized

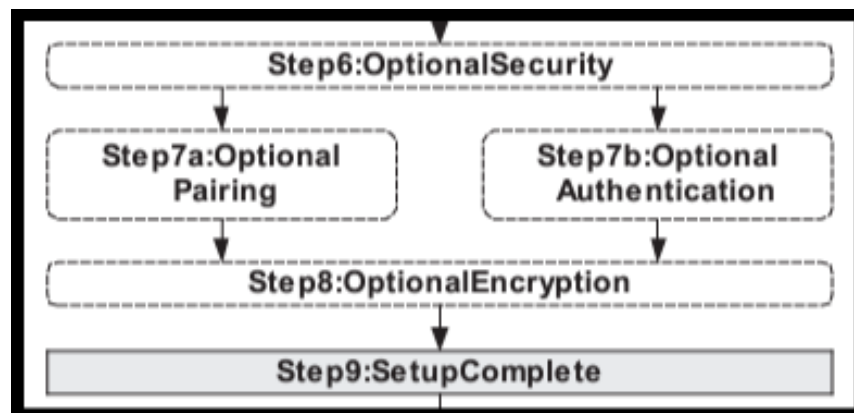
- Unpaired, unencrypted, authenticated, and unauthorized
- Unpaired, unencrypted, authenticated and authorized
- Unpaired, encrypted, unauthenticated and unauthorized **(default mode)**
- Unpaired, encrypted, unauthenticated and authorized
- Unpaired, encrypted, authenticated and unauthorized
- Unpaired, encrypted, authenticated, and authorized
- Paired, unencrypted, unauthenticated, and unauthorized
- Paired, unencrypted, unauthenticated, and authorized
- Paired, unencrypted, authenticated, and unauthorized
- Paired, unencrypted, authenticated and authorized
- Paired, encrypted, unauthenticated and unauthorized
- Paired, encrypted, unauthenticated and authorized
- Paired, encrypted, authenticated and unauthorized
- Paired, encrypted, authenticated, and authorized

123. As noted and discussed in detail above, in 2007 a POSITA would have understood that the Basic Imaging Profile (BIP) describes all the Kahn, Hiroishi, Feinberg, and Endsley scenarios. However, BIP did not require a paired Bluetooth connection for all these scenarios. For the scenarios most in line with Kahn,

Hiroishi, Feinberg, and Endsley, *i.e.* pull based or push based image transfer, BIP was not recommending using a paired Bluetooth connection.

124. As discussed above, NONE of the cited references (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default for any scenarios. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

125. Petitioner wrongly asserts that: “cryptographically authenticating the identity of phone 40 was a required to pair Hiroishi’s Bluetooth camera 50 and phone 40.” This is unsupported and incorrect. One can have a paired connection without being authenticated, and one can have a authenticated connection without being paired.



126. Hiroshi Does Not Disclose the “Cryptographically Authenticating Identity” Portion of the Limitation. And in Bluetooth specification both are independent and optional elements that can exist and perform without the other.

127. As noted above, in my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification or NOT go with the recommendation provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

128. The third glaring deficiency in his analysis is that Hiroshi or Kahn or Bluetooth does not support event notification for new data.

129. Petitioner asserts that the thumbnail sent in Hiroshi is an event notification: “Because thumbnails provide a straight-forward event notification to the user” and “Hiroshi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images).”

130. I am informed and understand that the parties agreed to the following constructions in the District Court:

“data signal notification(s)”	“an indication of the presence of newly acquired data”
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)

131. In Hiroshi (0083) it is clear that camera receives an instruction/request from the mobile to send a thumbnail. (“If no in Step 118, *i.e.*, when the instruction information received from the mobile phone 40 in Step 104 is not the thumbnail transmission instruction information, the process goes to Step 122”).

132. In Hiroshi Step 118, a mobile in a remote control mode sends a instruction request for a thumbnail to the camera, and the camera then responds by sending the requested thumbnail to the phone. It is simple request-response scenario.

133. In software design there are two very *different* categories of application architectures. **Request driven and Event Driven.**

134. A Request-Driven Architecture uses a **synchronous** request-response model where a component directly asks for information from another *and waits for a response* before proceeding. Request-Driven is more suitable for traditional client-server interactions where a direct response is required.

135. An Event-Driven architecture communicates between components by publishing and reacting to events, essentially working **asynchronously**. Event-Driven architecture is better for real-time, loosely coupled systems that need to react to events as they occur.

136. Key Differences are:

Communication Pattern for Event-Driven: Publishes/sends events that any interested component can subscribe/listen to and process it asynchronously.

Communication Pattern for Request-Driven: Sends direct requests to a specific component and waits for a response.

137. Support for these assertions can be found in Exhibit 2010 that has pages from three different books: (i) **2003 Book**, C# in a Nutshell ; By Peter Drayton, Ben Albahari, Ted Neward; (ii) **2006 Book**, **Event-Based Programming**, Taking Events to the Limit. By Ted Faison; and (iii) **2009 Book**, C# 3.0 in a Nutshell, A Desktop Quick Reference, By Joseph Albahari, Ben Albahari.

138. The Challenged Claims require Enabling “Event Notifications” and sending “Event Notification” to a listener without caring for a response from the listener, is completely different from the sending a “request and waiting for a response” architecture in BOTH Hiroshi and Kahn.

139. Moreover, the Challenged Claim uses plural for “enabling event notification(S)”. But when the claim is sending the event notification it is for single event “sending event notification”. Reaffirming that it is completely different from single request and single response architecture. Enabling event notifications is done **once** for multiple events to be received in the future. Unlike simple request response architecture. Petitioner’s argument conflates two vastly different scenarios, which a POSITA would not do.

140. Petitioner relies on the *thumbnail transmission instruction* as a purported “message to enable event notifications.” (“Hiroishi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images)”; “the mobile phone sends the camera a *thumbnail transmission instruction*, which is a message to enable event notifications corresponding to the new data”).

141. First, it is undisputed that Hiroishi clearly says that the referenced “*thumbnail transmission instruction*” is the information for instructing the transmission of the image data. See Hiroishi (Exh. 1011) at [0068] (“*Thumbnail*

transmission instruction information ... is the information for instructing the transmission of the image data showing the thumbnail of the image shown according to the digital image data stored in SDRAM 55A”). As such, it is plainly *not* “to enable event notifications.” (Plural Notifications not single request response).

142. Second, the “enablement of event notifications” as claimed is a single occurrence, and would not be characterized or satisfied by a transmission associated with each and every new image taken. Under Petitioner’s view; namely, that the transmission of thumbnail instructions is performed “to enable event notifications,” then the process of “enabling event notifications” would be required for every new image requested by the phone. This is plainly not the way in which a POSITA would understand “enabling event notifications” to work, and would wholly defeat the purposes of enabling event notifications in the first place.

143. A reasonable POSITA would have understood that a mobile device sending a “thumbnail transmission instruction” to the camera, followed by the receipt of the thumbnail, *is a simple request-response transaction* between the two devices that needs to be done *for each new thumbnail*. It is plainly *not* an “enabling of event notifications for the new data” by any means. (enabling plural number of notifications is NOT the same as single request response for thumbnail).

144. The word “event” or “event notification” itself does not exist in either Kahn or Hiroshi. This is unsurprising, given the fact that both those state machines are based on request-response architecture. For example, ALL instructions follow the same request-response pattern in Hiroshi and Khan. The phone sends an instruction to the camera and then waits for a response. *See* Hiroshi at [0092-93]: “In Step 206, image transmission start instruction information is transmitted via the communication unit 49 to the digital camera 50. In response to this, the digital camera 50 performs Step 108 of the digital camera processing (also see FIG. 5) to start an image transmission processing. So, in the following Step 208, [the phone] waits for the reception of the digital image data transmitted from the digital camera 50,”

145. As illustrated in the annotated Figure below (*see* Hiroishi (Exh. 1011) at Fig. 5, as annotated), the process of Hiroishi simply calls for a sequence of instructions sent from the mobile device to the camera:

the key difference is that request-response is a direct, *synchronous* communication while event notification is a broadcast-like, *asynchronous* communication where the receiver decides when to act upon the information. Support for these assertions can be found in the Exhibit 2010.

148. In request-response, the client initiates communication by sending a request. In event notification, the system generates an event that triggers the notification. Request-response is synchronous, meaning the client waits for the server's response before continuing. Event notification is asynchronous, meaning components can react to events at their own pace. Under that architecture, the mere receipt of a reply to an instruction/request in Hiroshi cannot be reasonably understood as an "event notification" as claimed.

149. Petitioner initially relies on the *thumbnail transmission* as a purported event notification. More specifically, Petitioner asserts that the thumbnail sent in Hiroshi is an event notification: "a thumbnail and/or data related to the thumbnail would operate as a notification signal," and "transmission of thumbnails as event notifications." In my opinion, Petitioner's position is untenable, inasmuch as **there is nothing in Hiroishi that performs as an event notification.** Again, Step 118 of receiving a request from the mobile to send a thumbnail and then camera sending the thumbnail to the mobile is NOT an event notification, in any sense of the word for a POSITA.

150. Petitioner fails to appreciate that in any application data model, you have to follow **either** request-response or event-based notification. Here the Petitioner seeks to combine two orthogonal data architectures. One does not “wait for a response” in an “event notification” architecture. Nevertheless, Petitioner acknowledges and asserts that Hiroshi is “waiting for a response” which, by definition, is not an “event notification.” Because in Event Notifications there is NO waiting for a response. Simply put, Hiroshi has very little in common with the teachings and claims of the ‘030 Patent.

151. Petitioner further takes the position that the “waiting” component of Hiroshi “enables event notification listening” for event notifications that are for new data. On inspection, a POSITA would readily appreciate that the application of the “wait” in Hiroshi varies throughout the disclosure, but in no sense is it *ever* used to define any act of enabling event notification listening. *See* Hiroshi (Exh. 1011) at [0002] (“... waits for the shutter to release”); at [0073] (“... [the camera] waits to receive the instruction information from the mobile phone”); at [0091] (“... [the phone] waits for an operator to specify a desired mode”); at [0093] (“... [the phone] waits for the reception of the digital image data transmitted from the digital camera”); at [0097] (“... [the phone] waits until an operator presses any key”); at [0104] (“...[the phone] waits until it receives the image data that can display the thumbnail”); at [0106] (“... [the phone] waits for the end of selection of

the desired image”); at [0107] (“... [the phone] waits for the reception of the digital image data”); and at [0111] (“... the device waits for the operator to finish entering each information”).

152. Plainly, the act of merely “waiting” on an event to occur, as described in Hiroishi, cannot reasonably be understood to convey an “*enabling event notification listening* on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device” corresponding to existence of new data. Again, simply waiting for a response to an earlier instruction is *not* an enabling of event notifications for new data.

153. A POSITA would know and appreciate that every file that is created on a computer or camera or phone has a timestamp. And a POSITA would further know that a timestamp inside a file is not an event notification in any sense of the word.

154. Neither Hiroshi nor Kahn has been configured to “listen” to those timestamps. Receiving a file that you requested and that every file has timestamp is not “listening” for a timestamp, as any POSITA would recognize.

155. The word “event” or “event notification” itself is not found in either Kahn or Hiroshi. This is unsurprising, given the fact that both those state machines are based on request-response architecture. A “request-response” model involves a client actively sending a specific request to a server and waiting for a direct

response, while an “event notification” is a message sent out when a significant event occurs in a system, allowing any interested components to react *asynchronously* without needing to explicitly request the information. Support for these assertions can be found in Exhibit 2010.

156. As noted and discussed in detail above, under proper construction, it is very clear (including based on Exhibit 2010) that waiting for a response is outside of the meaning of the claim term “listen[ing]” for “event notification.”

157. Still further, Petitioner makes the curious argument that the “Sniff Mode” described in the Bluetooth Specification somehow illustrates a form of “sending a message to enable event notifications.” The deficiencies in this argument are many, but primarily it must be recognized that “Sniff Mode” (as defined in the Bluetooth Specification) is clearly a Layer 2 feature (LMP Link Manager Protocol), and has *nothing* to do with sending a message from the mobile device to the camera for enabling event notifications. LMP_Snif_req and LMP_unsnif_req have nothing to do with new data event notification. *See, e.g.,* Bluetooth Specification (Exh. 1019) at 456, as excerpted and annotated below.

When the ACL logical transport is in **sniff mode** the master shall only start a transmission in the sniff slots. Two parameters control the listening activity in the slave: the sniff attempt and the sniff timeout. The sniff attempt parameter determines for how many slots the slave shall listen when the slave is not treating this as a scatternet link, beginning at the sniff slot, even if it does not receive a packet with its own LT_ADDR. The sniff timeout parameter determines for how many additional slots the slave shall listen when the slave is not treating this as a scatternet link if it continues to receive only packets with its own LT_ADDR. It is not possible to modify the sniff parameters while the device is in **sniff mode**.

M/O	PDU	Contents
O(7)	<u>LMP_sniff_req</u>	timing control flags D _{sniff} T _{sniff} sniff attempt sniff timeout
O(7)	<u>LMP_unsniff_req</u>	-

Table 4.28: **Sniff mode** PDUs

Sniff Mode is a Layer 2 concept and is used to reduce power

- 1. It has *Nothing to do* with Event Notification for new images!**
- 2. It has *Nothing to do* with Enabling Event Notifications**

**LMP_sniff_req and LMP_unsniff_req
LMP Stands for “Link Manager Protocol”**

26 July 2007

Procedure Rules

158. As a POSITA would recognize, mobile applications don’t even have access to hardware level Link Layer (layer 2) LMP Link Manager Protocol. *See also id.* at 386 and 395 (as excerpted and annotated below):

Sniff mode	This feature indicates whether the device is able to support sniff mode as defined in baseband Section 8.7 on page 175 using the LMP sequences defined in Section 4.5.3 on page 286 .
Sniff subrating	This feature indicates whether the device is able to support sniff subrating as defined in [PART B] Sniff Subrating on page 177 using the LMP sequences as defined in Sniff Subrating on page 288 . This feature bit shall be set if the " Sniff mode " feature bit is set.
Park state	This feature indicates whether the device is able to support Park state as defined in baseband Section 8.9 on page 179 using the LMP sequences defined in Section 4.5.2 on page 279 .

Table 3.1: Feature Definitions

26 July 2007
Device Features

386

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2]
page 225 of 906

Link Manager Protocol

mode or park state, the initiating LM shall perform the procedure to exit **sniff mode** or park state before initiating the procedure defined above. If the procedure to exit **sniff mode** or park state does not complete within the LMP response timeout (30 seconds) the procedure defined above shall be initiated anyway.

```

sequenceDiagram
    participant A as initiating LM
    participant B as LM
    A->>B: LMP_detach

```

Sequence 1: Connection closed by sending LMP_detach.

159. A POSITA would understand that Bluetooth Sniff Mode messages have nothing to do with event notifications, and Bluetooth Sniff Mode has nothing to do with new data/photos being taken by the camera. **The term “Event Notification” does not exist in the Bluetooth 2.1 Specification.**

160. The fourth glaring deficiency is that “object” and “file” are NOT the same. While Claims 6 and 15 recite creating an “Object,” the regular file with a timestamp of Hiroshi or Khan **cannot** be considered as an “Object.”

161. Petitioner asserts that: “Takahashi discloses that the new data picture is saved in a file along with a first timestamp of the time the picture was taken,” and further that: “Kahn teaches that “the image data already includes timestamp information (*i.e.*, timestamp indicating when the image is captured).”

162. As noted and discussed in detail above, the term “object” is also disputed by the parties in the District Court case, and that Cellspin proposes the following: “An object can be a variable, a data structure, a function, or a method. Object contains value and is referenced by an identifier.” I agree with this construction.

163. As further noted and discussed in detail above, the evidence clearly shows that an Object is different from a File. As further discussed in detail above, a POSITA would readily appreciate the fact that a “file” has to be converted to be an “Object” to be sent using OBEX. Similarly, “Data” (that is NOT itself a “File”) can also be converted into an Object and then sent/transferred using OBEX protocol. OBEX is an **object exchange** protocol, **NOT** a file exchange or data

exchange protocol, but both file and data can be sent using it by creating an Object first.

164. The fifth glaring deficiency is that (assuming “along with” is properly construed), Takahashi *does not* teach sending User Identifier “Along With” the New Data.

165. As noted and discussed in detail above, the term “along with” should be construed as “in addition to,” and which expressly excludes simply “inside.”

166. Petitioner argues that combinations involving the Takahashi reference (Exh. 1014) obviate the Challenged Claims. One primary use of Takahashi, according to Petitioner, is its disclosure of the User ID with the file name. Indeed, Petitioner claims: “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.” Petitioner also argues: “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.” (citing Takahashi at [0066] (“user ID in the file name of image data”)).

167. These teachings of Takahashi, however, do not satisfy the “along with” limitation which, as discussed above, is “in addition to.” **As taught in Takahashi, the User ID is part of the filename, not an identifier transmitted “in addition to” the new data.**

2. Ground 1B – Hiroishi in Combination with Kahn and Bluetooth V2.1

168. David Lett suggests that a POSITA would have been motivated to combine the teachings of Hiroishi in Combination with Kahn and Bluetooth 2.1 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

169. First, as required, and as shown above, I have examined the scope and content of the cited prior art. With respect to teachings of Hiroishi, Kahn, and Bluetooth V2.1, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Hiroishi in combination with Kahn and Bluetooth V2.1 reference render the Challenged Claims obvious. I disagree David Lett's conclusions. Here, I address the most glaring deficiencies in his analysis.

170. As an initial point, the main reason Petitioner relies on Kahn is for HTTP and "object creation" support.

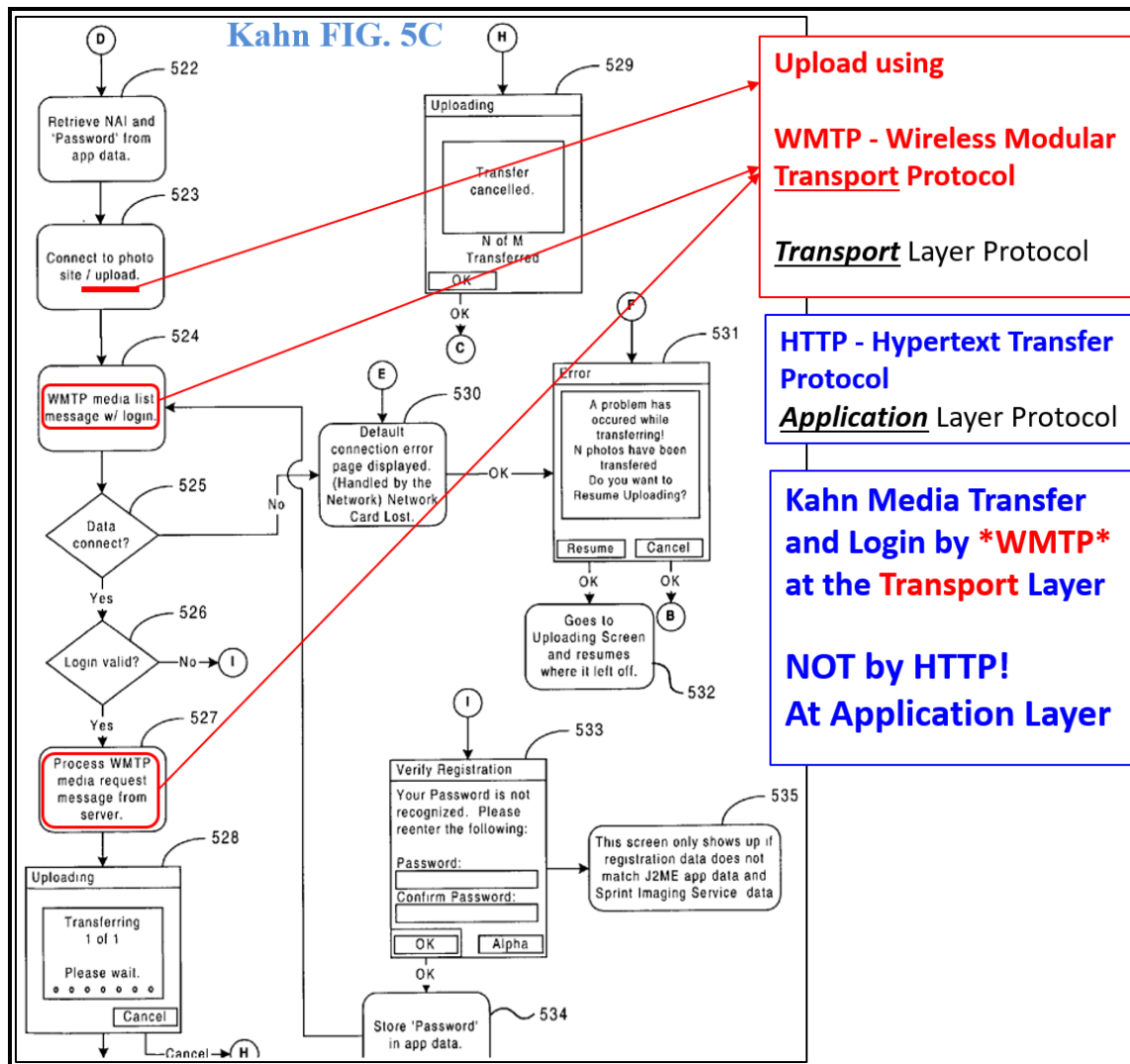
171. As discussed in detail above, a File is different from an Object, and this same reasoning applies the timestamp of Kahn. As a POSITA would recognize, every computer file has a timestamp. In any event, Kahn does *not* teach sending user information and user data (photos/media) using HTTP.

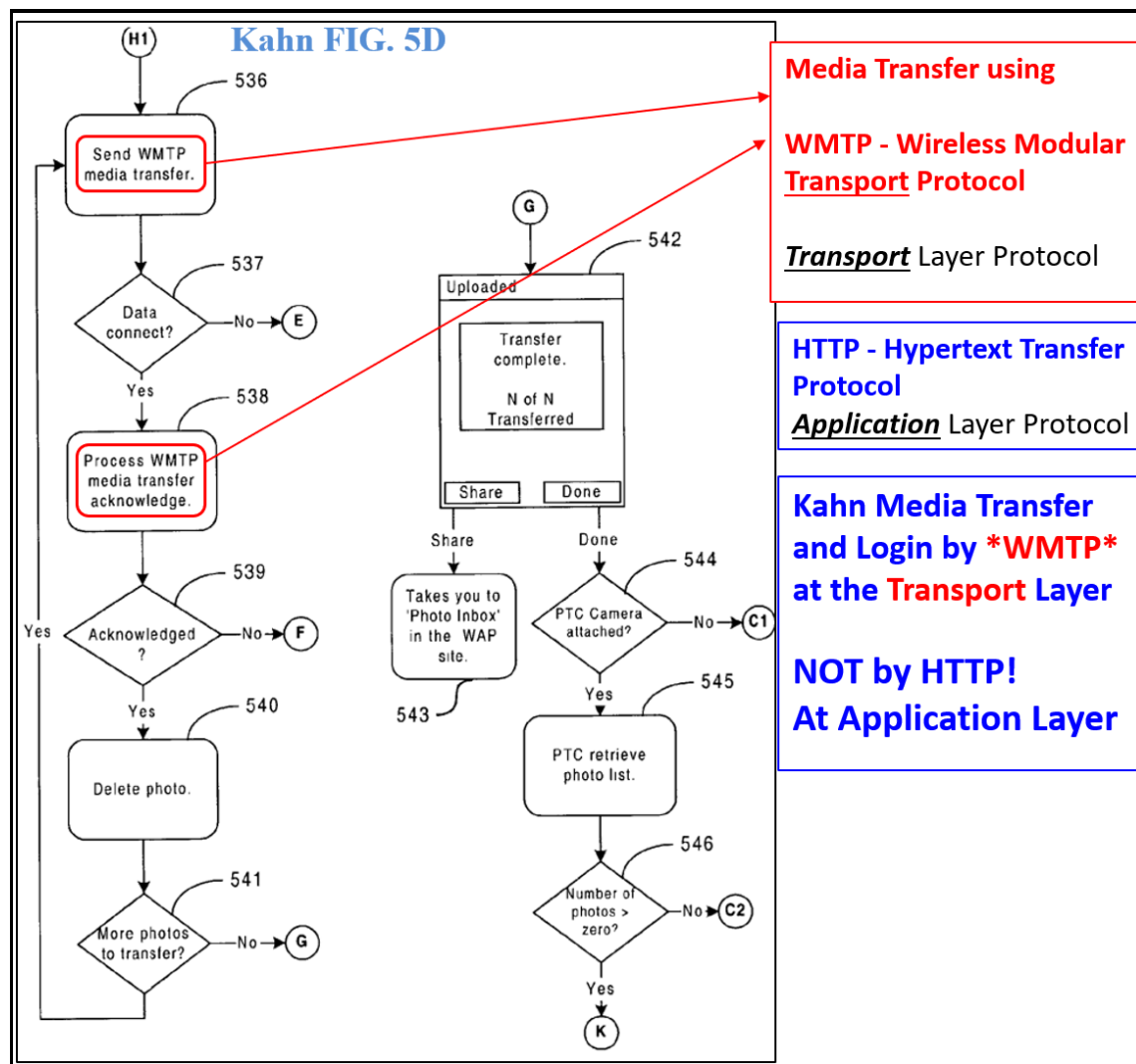
172. The big glaring deficiency is that Kahn does NOT teach use of HTTP for uploading photos/media. Instead, Kahn required using WMTP for media

upload. However, a POSITA would recognize the fact that HTTP and WMTP are NOT interchangeable.

173. Wireless Application Protocol (WAP) and Wireless Modular Transport Protocol (WMTP) are the wireless communication technique (circa 2004), and Hyper Text Transfer Protocol (HTTP) is the *standard protocol for the web*. When Kahn says the upload process “occurs via wireless communication technique,” it is in reference to wireless WAP and wireless WMTP protocols (*not* HTTP).

174. It is very clear with respect to **media transfer and login** that Kahn teaches the *exclusive use of WMTP*. See Kahn Fig 5C and Fig 5D as reproduced below:





175. Kahn [0057] makes it even more clear that the **Wireless** Modular Transport Protocol (WMTP), a wireless communication technique, is exclusively used for uploading. See Kahn at [0057]: “[T]he *uploading process occurs via wireless communication technique*, with the local host (e.g., cell phone, wireless PDA, or the like) assuming responsibility for establishing a wireless data connection.” As taught by Kahn, a POSITA is to use WMTP as described in Fig

5C and Fig 5D. It is understood that WMTP is a wireless protocol and HTTP is and was a web protocol.

176. Kahn Fig 5D, **element 543**, also mentions another wireless communication technique: WAP (**Wireless** Application Protocol). In 2004 (the time of Kahn), the industry was pushing for wireless protocols like WAP and WMTP (**Wireless** Modular Transport Protocol) for wireless mobile device for web access. WAP and WMTP were specifically designed for mobile devices with limited bandwidth, with WAP acting as a gateway to translate requests from a mobile phone into standard HTTP requests, whereas HTTP (Hypertext Transfer Protocol) is the standard protocol used for web browsing on traditional computers. WMTP and WAP were particularly relevant in the early days of mobile internet when data capabilities were significantly lower.

177. When Kahn references “wireless communication techniques” in [0057] for “uploading,” it very clearly shows two wireless protocols WMTP and WAP in Fig 5D. It is thus clear that Kahn wants to use wireless protocols like WMTP for upload and NOT web protocol HTTP.

178. I understand that, in its Institution decision relating to the '121 Patent (at page 41), the Board mentions that: “While the term ‘WMTP’ appears in these figures, it does not seem to be defined or discussed elsewhere in Kahn.”

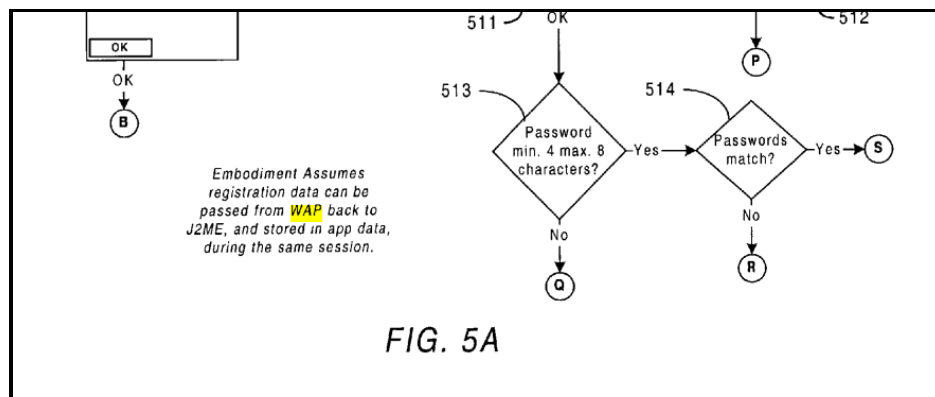
179. The reason for this is because Kahn assumes the POSITA knows about WAP architecture and usage in the wireless domain. Just like a POSITA for the wired network would know about TCP/IP or OSI stack, Kahn assumes the POSITA is knowledgeable about the WAP architecture and WMTP in the WAP system. Indeed, Kahn talks about wireless transmission techniques and in the detailed diagrams it mentions WMTP and WAP.

180. In a WAP (Wireless Application Protocol) architecture system, the “wireless modular transport protocol” (WMTP) refers to the Wireless Datagram Protocol (WDP), which acts as the transport layer within the WAP stack, providing a flexible way to transfer data across different network types, even when dealing with unreliable or limited bandwidth connections typical in mobile networks; essentially acting as a modular adaptation layer for various underlying bearer services.

181. Again, it is clear that Kahn intends for the POSITA to use WAP architecture and system. **Kahn talks in great detail about WAP and WAP specification in [0017]** and assumes POSITA to know about WAP architecture, and WAP usage in the wireless domain (WMTP being the transport layer protocol in the WAP architecture in 2004). *See* Khan at [0017]: “**WAP**: Short for the Wireless Application Protocol, a Secure Specification that allows users to access information instantly via handheld wireless devices Such as mobile phones, pagers,

two-way radios, ‘Smart’ phones, and communicators. WAP uses WML or ‘Wireless Markup Language’ which is a tag-based display language providing navigational Support, data input, hyperlinks, text and image presentation, and forms, it is a browsing language Similar to Internet HTML. **WAP supports most wireless networks**, including CDMA and GSM. The **WAP 2.0 specification** is available from Open Mobile Alliance, Ltd.”

182. Further, WAP is also described in Kahn **Fig 5A**, and it is clear that in Kahn 5A, WAP is used to connect the mobile app (J2ME Applet in 2004) to the outside internet for login registration and password. It is NOT HTTP, but WAP that is used for login password and registration:



183. WAP is also described in Kahn **Fig 5G**, which talks about user account that is a “user’s WAP Account.” This is plainly not an HTTP account.

Glossary for J2ME App	
Yes-	Confirms action and takes user to next screen
No-	Cancels action and takes user back to previous screen
OK-	Confirms action and takes user to next screen
Done-	Completes task and takes user to initial page
Cancel-	Cancels action and takes user to previous screen
Exit-	Exits application
Upload-	Initiates transfer of selected photo to user's account
Upload All-	Initiates transfer of all photos to user's account
Delete-	Removes selected photo from camera
Delete All-	Removes all photos from camera
Preview-	View photos in camera
Share-	Closes J2ME app and launches to user's WAP account
Next-	Displays next photo
Prev-	Displays previous photo

FIG. 5G

184. In 2004, WAP (Wireless Application Protocol) was considered better than HTTP (Hypertext Transfer Protocol) for mobile devices due to several reasons:

- 1. Optimized for Mobile Devices:** WAP was specifically designed for the limited capabilities of mobile devices at the time, such as small screens, low memory, and limited processing power. It used WML (Wireless Markup Language) instead of HTML, which was more suitable for mobile displays.
- 2. Efficient Use of Bandwidth:** WAP was optimized for narrow-band bearers with potentially high latency, making it more efficient in terms of bandwidth usage compared to HTTP. This was crucial for mobile networks, which had slower data speeds and higher latency.

3. Security: WAP included Wireless Transport Layer Security (WTLS), which provided a public-key cryptography-based security mechanism similar to TLS. This was important for ensuring secure communication over potentially unprotected mobile networks.

4. Adaptation to Wireless Networks: WAP was designed to work with various wireless data networks, such as GSM and CDMA, and included protocols like Wireless Datagram Protocol (WDP) and Wireless Transaction Protocol (WTP) that were adapted to the wireless environment. *These features made WAP more suitable for the mobile internet experience in that timeframe.*

185. Kahn [0056] does talk about using HTTP to communicate with the image server, BUT it is for Ecommerce purpose. This whole text of [0056] where HTTP is mentioned is about the cellphone taking to an image server for e-commerce and processing fulfilment or ordering hardcopies and enlargement. In any event, in Kahn [0056] there is no mention of using HTTP to upload photos.

186. Kahn [0062-0063] is another example of Kahn talking about using HTTP for **internal communication** within the Cellphone with hardware GPS chip by Qualcomm SnapCore that is inside the phone itself, by using location API. Here HTTP is being used within the host/cellphone to communicate with the hardware chip *SnapCore* to get GPS data from the hardware Chip that resides

inside the phone itself. The Location API call is **not** going out to the server on the internet, it is to-and-from the Qualcomm chip on the phone.

187. In sum, Kahn is very clear to the POSITA on what protocols to use and where. Specifically: HTTP for e-commerce and internal hardware chip location API. As for uploading/media-transfer and login information, on the other hand, Kahn is very clear to POSITA to use WMTTP.

188. Petitioner's assertion that POSITA would use HTTP instead of the clear teaching of WMTTP in Kahn for uploading/media-transfer/login is not supported at all in Kahn, and does not reflect the approach to be taken by a POSITA.

189. **Moreover, WMTTP and HTTP are very different protocols and they are NOT Interchangeable.** A POSITA would understand and appreciate that both WMTTP and HTTP run on different layers of the OSI stack. They are NOT interchangeable and there are significant differences between these two protocols. The key difference lies in their primary purpose and application domain: HTTP (Hypertext Transfer Protocol) is the standard protocol for web browsing and data transfer on the internet, while Wireless Modular Transport Protocol (WMTTP) is specifically designed for communication between devices within a wireless modular network, often used in industrial scenarios where reliability and low latency are critical. *See <https://ieeexplore.ieee.org/document/4689157>.*

Abstract:

A new modular transport layer protocol for wireless sensor networks (WSNs) is proposed: WMTP - Wireless Modular Transport Protocol. This protocol not only allows the simultaneous use of all the main features commonly found in WSN transport protocols, namely congestion-control, fairness, and reliability, but also does so in a modular fashion. This way, the application layer can choose to use exactly the features that it requires. Additionally, WMTP also provides a set of uncommon features such as throttling, flow-control, transport layer quality- of-service, and optional integration with service-discovery. Focusing specifically on the fairness feature, experimental results show that the network resources are appropriately divided whether a simple fairness semantic is used, or in the presence of weighted differentiation. Additionally, this feature is shown to operate with minimal energy cost, as the protocol overhead is less than 10%.

190. There are a number of clear differences between HTTP and WMTP.

Among them are the following:

Key points about HTTP: It is at the *seventh layer* of standards in (OSI) reference model. *Function:* Primarily used for transferring web pages and data between web servers and client devices like web browsers. *Request-Response model:* Operates on a clear request-response mechanism where a client sends a request to a server and receives a response. *Adopted:* as the standard protocol for web communication.

Key points about WMTP: It is at the *fourth layer* of standards in (OSI) reference model. *It Focus on wireless networks:* Designed to facilitate reliable communication between devices within a wireless modular network, often in industrial settings. *Low latency and reliability:* Prioritizes fast data transfer with high reliability, crucial for real-time control applications. *Specialized use case:* Not as widely used as HTTP, primarily

targeted towards applications where devices need to communicate wirelessly in a controlled environment.

Functionality of Transport layer protocols and Application layer

protocols are very different. Function of Transport layer protocols like WMTP, TCP, UDP is to manage data segmentation, error checking, and flow control. Function of application layer protocols like HTTP, FTP is to define the structure and content of data for specific applications.

Abstraction level needed and required for both WMTP and HTTP is very different. The transport layer operates at a lower level providing a reliable communication channel. Application layer operates at a much higher layer, allowing applications to focus on their specific tasks without worrying about network complexities.

191. The reason POSITA will not go against teaching of Kahn for using WMTP and switching to HTTP is because the two protocols are NOT Interchangeable. It is not like switching from FTP to *Secure* FTP. It is even not like switching from FTP to HTTP where both are at the application layer protocol (not recommended).

192. In sum, HTTP is application layer protocol that is the standard for web-based data transfer, while WMTP is a specialized transport layer protocol for wireless communication in specific industrial environments, emphasizing

reliability and low latency within a dedicated network. They are NOT Interchangeable.

- 3. Ground 2A – Singh 129 in View of Bluetooth**
- 4. Ground 2B – Singh 129 in View of Bluetooth and Takahashi**

193. David Lett suggests that a POSITA would have been motivated to combine the teachings of Singh 129 in view of Bluetooth 2.1 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

194. First, as required, and as shown above, I have examined the scope and content of the cited prior art. With respect to teachings of Singh 129 and Bluetooth 2.1, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Singh 129 in combination with Bluetooth 2.1 reference render the Challenged Claims obvious. I disagree David Lett's conclusions. Here, I address the most glaring deficiencies in his analysis.

195. For both Grounds 2A and Ground 2B, I understand that Petitioner has raised § 112 issues regarding three claim elements of the '030 Patent, and specifically, I understand Petitioner alleges that there is a purported lack of support in the specification for: (i) 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; (ii) include a timestamp in with the new data object; and (iii) encrypt/decrypt the data.

196. I will address all three of them below.

197. First it is noted that the Patent Examiner did not raise any § 112 objections for any of the three issues Petitioner has now raised. In my opinion, this is unsurprising, given the fact that each of these limitations are disclosed in the specification.

198. **FIRST:** Petitioner complains about sending/receiving messages to negotiate “supported data capability” for claim 1 and 12.

199. It would have been well known to a POSITA that “Handshake Protocol” is used for communicating / negotiating the data-and-other capabilities from one device to another device.

200. In this regard, the specification is very clear about implementing the *handshake protocol*: “**By implementation of a handshake protocol**, the BT communication device **201** *a* automatically transfers captured data, the multimedia content, and the associated files to the client application **203** on the mobile device **202.**” See ’030 Patent at 4:59-62.¹

201. The claim limitation Petitioner is complaining about was suggested, proposed, and added by the Examiner himself during the **Examiner Initiated Interview**. (Page 30,31 and 44 of Exhibit 2011):

¹ The ’030 Patent specification will be used as a reference for the written description throughout (unless noted otherwise), as it contains the same disclosure for all 7 Challenged Patents.

Examiner-Initiated Interview Summary	Application No. 14/295,353	Applicant(s) SINGH ET AL.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2478	

All participants (applicant, applicant's representative, PTO personnel):

(1) SULAIMAN NOORISTANY. (3) _____.

(2) Ashok Tankha (Reg. # 33,802). (4) _____.

Date of Interview: 23 September 2014.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: _____.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant agreed that the examiner's amendment, authorized by the above attorney, would place the application in condition for allowance.

Examiner Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ashok Tankha (Reg. # 33,802) on 9/23/2014.

Claims Are Amended As Follows:

CLAIMS:

Claim 1 (Currently Amended): A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

performing at a Bluetooth enabled data capture device:

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;

acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;

202. Below are the excerpts from three different sources about what *handshaking* and *handshake protocol* entails, as well as what a POSITA understands the handshake protocol to be. These sources are: (i) A 2007 Book:

“PC-BASED INSTRUMENTATION, CONCEPTS AND PRACTICE, By N. MATHIVANAN” (Page 383); (ii) Wikipedia page about handshake protocol; and (iii) (2002) Microsoft Computer Dictionary Fifth Edition (page 245).

203. First, the 2007 book clearly shows what “handshake protocol” is (as well as how it would have been understood by a POSITA), and it is being used to exchange supported data “capabilities of a device”. (EXHIBIT 2012) *See* www.google.com/books/edition/PC_BASED_INSTRUMENTATION/OB65rMNQDo8C?hl=en&gbpv=

Table 8.2 GPIB capabilities, their symbols and functional descriptions

Interface capability Symbol Function		Description
T	Talker	Capability of a device to talk.
TE	Extended Talker	Capability of a talker to extended addressing.
L	Listener	Capability of a device to listen.
LE	Extended Listener	Capability of a listener to extended addressing.
SH	Source Handshake	Capability of a device to send command or data byte (multiline message) over GPIB using the three-wire handshake protocol.
AH	Acceptor Handshake	Capability of a device to receive command or data bytes (multiline message) from GPIB using the three-wire handshake protocol.
RL	Remote/Local	Capability of the device to switch between response to its front panel controls and response to commands sent over GPIB.
SR	Service Request	Capability of a device to assert service request to obtain service from controller.
PP	Parallel Poll	Capability of device to indicate that it needs service when the controller requests the status.
DC	Device Clear	Capability of a device to be reset.
DT	Device Trigger	Capability of a device to be triggered by a GPIB command to perform a device dependent function.
C	Controller	Capability of a device to send addresses, universal commands and addressed commands to other devices on the bus. It also includes the capability of the device to conduct polling to determine a device requesting a service.
E	Drivers	It describes the type of electrical bus drivers used in the device.

The IEEE-488 further defines subset of the above capabilities by a number appended to the capability symbol. The standard recommends that the GPIB capabilities of a device be symbolically marked near the GPIB connector on each device to indicate the interface functions the device supports. For example, the symbolic code 'SH1, LH1, T6, L4, SR1, RL1, PP0, DC1, DT0, C0, E2' indicates that the device has the following GPIB capabilities.

- (a) SH1 : Capability to transmit multiline messages across GPIB.
- (b) LH1 : Capability to receive multiline messages from GPIB.
- (c) T6 : Capability to become a talker when talk address with ATN asserted is sent by controller on the bus. Capability to respond to serial poll. The device ceases to be a talker when talk address of another device with ATN asserted is sent by the controller on the bus. The device does not have the talk-only capability.
- (d) L4 : Capability to become a listener when a listen address with ATN asserted is sent by controller on the bus. The device does not have the listen-only capability.
- (e) SR1 : Capability to assert SRQ line when the device requires a service.
- (f) RL1 : Capability to respond to both Go To Local (GTL) and Local Lock Out (LLO) command messages.
- (g) PP0 : Does not have the capability to parallel poll.
- (h) DC1 : Capability to respond to Device Clear (DCL) and Selected Device Clear (SDC) command messages.

204. Second, Wikipedia states: “Handshaking can negotiate parameters that are acceptable to equipment and systems at both ends of the communication channel, including **information [data] transfer rate**, coding alphabet, parity, interrupt procedure, and other protocol or **hardware features**.” See [en.wikipedia.org/wiki/Handshake_\(computing\)](http://en.wikipedia.org/wiki/Handshake_(computing)).

In computing, a **handshake** is a signal between two devices or programs, used to, e.g., authenticate, coordinate. An example is the handshaking between a [hypervisor](#) and an application in a [guest virtual machine](#).

In [telecommunications](#), a **handshake** is an automated process of negotiation between two participants (example "[Alice and Bob](#)") through the exchange of information that establishes the protocols of a communication link at the start of the communication, before full communication begins.^[1] The handshaking process usually takes place in order to establish rules for communication when a [computer](#) attempts to communicate with another device. Signals are usually exchanged between two devices to establish a communication link. For example, when a computer communicates with another device such as a [modem](#), the two devices will signal each other that they are switched on and ready to work, as well as to agree to which protocols are being used.^[2]

Handshaking can negotiate parameters that are acceptable to equipment and systems at both ends of the communication channel, including [information transfer rate](#), coding [alphabet](#), [parity](#), [interrupt](#) procedure, and other [protocol](#) or hardware features. Handshaking is a technique of communication between two entities. However, within TCP/IP RFCs, the term "handshake" is most commonly used to reference the TCP three-way handshake. For example, the term "handshake" is not present in RFCs covering FTP or SMTP. One exception is Transport Layer Security, TLS, setup, FTP RFC 4217. In place of the term "handshake", FTP RFC 3659 substitutes the term "conversation" for the passing of commands.^{[3][4][5]}

205. Third, the Microsoft Computer Dictionary Fifth Edition (page 245) defines “handshake” as: “**A series of signals acknowledging that communication or the transfer of information.**”

handshake *n.* A series of signals acknowledging that communication or the transfer of information can take place between computers or other devices. A hardware handshake is an exchange of signals over specific wires (other than the data wires) in which each device indicates its readiness to send or receive data. A software handshake consists of signals transmitted over the same wires used to transfer data, as in modem-to-modem communications over telephone lines.

245

206. There are various handshake protocols depending on the application. The most common are the “three-way handshake” or “4-way handshake” protocol

that are used to negotiate data capabilities, security parameters and more. TCP/IP communication between devices uses handshake protocol before data transfer, SSL/TLS uses handshake protocol for negotiating security parameters, wireless protocol like WPA/WPA2 use four-way handshake for negotiating authentication parameters and other things.

207. Below is another example of SSL/TLS uses handshake protocol for negotiating security parameters from the 2006 Edition of the Information Security Management Handbook. *See* www.google.com/books/edition/Information_Security_Management_Handbook/5sIJ4Ho5yLUC?hl=en&gbpv=1&kptab=getbook

Understanding the TLS Handshake Protocol

The TLS Handshake Protocol allows two peers to agree upon security parameters for the TLS Record layer, authenticate, initiate those negotiated security parameters, and report errors to each other.

During the session negotiation phase, the Handshake Protocol on each peer negotiates the security parameters in Table 6.1.

Once the session is initiated, however, the application can request a change in the cryptographic elements of the connection. The change is handled through the "change cipher spec protocol," which sends a message to the peer requesting a change to the cipher properties. The change itself is encrypted with the current cipher values to ensure the request and associated information cannot be deciphered if intercepted.

How the Protocol Works

For TLS to properly protect a session using cryptographic features, it must negotiate the cryptographic parameters. Figure 6.2 illustrates establishing the session.

Upon initiating a TLS connection, the two nodes must establish a "handshake" and negotiate the session parameters. These parameters include the cryptographic values, optional authentication, and generated shared secrets.

Dissecting the Handshake Protocol

When the client contacts the server to establish a connection, the client sends a client hello message to the server. The server must respond with a server hello message or the connection fails. This is extremely important, as the hello messages provide the security capabilities of the two nodes.

Specifically, the hello message provides the following security capabilities to the other node:

- TLS protocol version
- Session ID
- Available cipher suite
- Compression method

As mentioned, both nodes compute a random value I that is also exchanged in the hello message.

Exchanging the keys can involve up to four discrete messages. The server first sends its certificate, provided the server is to be authenticated. If the certificate is only for signing, the server then sends its public key to the client. The server then sends a “server done” message, indicating that it is waiting for information from the client.

© 2006 by Taylor & Francis Group, LLC

Copyrighted material

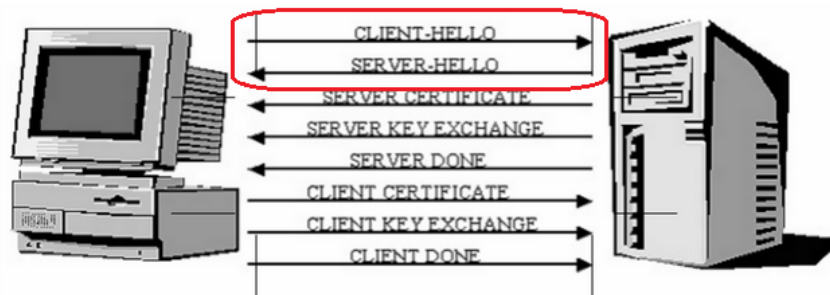


FIGURE 6.3 Handshake exchange.

208. A POSITA in 2007 clearly knew that the handshake protocol is to negotiate parameters such as data capabilities. As such, the specification’s disclosure of “implementing a Handshake Protocol” tells that messages are sent and received for data and other capabilities. The disclosure supports the claim limitations for a POSITA about sending messages to negotiate “supported data capability” for claim 1 and 12.

209. Next, Petitioner complains about support for “timestamp in the data Object” for Claim 15, which recites: “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.”

210. Petitioner does NOT complain about Object being created with data and associated data. The Object is being transferred by using OBEX, as explained in the specification: “The digital data capture device 201 then automatically **transfers** 106 the captured **data**, the **multimedia** content, and the **associated** files to the client application 203 on the mobile device 202 using one or a combination of file **transfer protocols**. The file transfer protocols may, for example, be one or a combination of BT profile protocols such as the **object exchange (OBEX) protocol**, the generic object exchange profile (GOEP) protocol, etc.” *See* ’030 Patent at 4:34-41.

211. Petitioner fails to realize that when the Object is created for OBEX transfer/exchange, “Time” is one of the headers in the OBEX object. A POSITA also knows that **OBEX has a timestamp header** that is filled when the data object or file object is created. *See* Exhibit 2009 (IrDA - OBEX Version 1.3 Document - *Page 73*):

9.2 Generic File Object

9.2.1 Introduction

The purpose of this chapter is to outline a method for the exchange of a basic file object [blob] from one device to another. While the OBEX protocol provides many useful headers and capabilities for exchanging objects. This section is designed to provide the reader with an overview of the basic structure used when exchanging generic file data. The file object is assumed to be sent by a generic client to the receiving device's inbox. In a manner consistent to the way QuickBeam and IrXfer applications work. Based on these assumptions, the file exchange should follow the guidelines shown here for headers used and response codes expected.

9.2.2 Commonly Used Headers

- **Name:** *(Required)* This header is used to convey the full name of the object to exchange. The **Name** header should not contain any path information. If it is necessary to specify a path, it should be done with the **SETPATH** command. All information in this header is interpreted as the objects name.
- **Length:** *(Recommended)* This header is used to convey the size of the file object in bytes. This can be used for verification of storage space requirements. The sum of the bytes passed in **Body** headers should be this many bytes (but is not guaranteed).
- **Body/End-of-Body:** *(Required)* Body headers are used to transfer the file data itself. They are sent repeatedly as long as file data exists to be exchanged. The **End-of-Body** header is used to indicate to the receiving application that this is the last piece of the file data. Applications frequently close the file and consider the transfer complete upon reception of this header. The data contained in the **Body/End-of-Body** headers should be concatenated to form the file.
- **Time:** *(Recommended)* This header is used to exchange the time that the file was last modified. Current file transfer applications use both the simple 4-byte **Time** header and the ISO format. It is recommended that all applications use the more robust ISO **Time** header. For backward compatibility it should be noted that the "IrXfer" application provided by Microsoft only accepts the 4-byte **Time** header. Attempts to send the ISO header will result in the rejection of the operation.
- **Type:** *(Optional)* The MIME type of the file object. This is not often used but can be helpful in some cases to identify the application to associate with the file object.

9.2.3 Response Codes Commonly Used in File Exchange

The following is a list of the known OBEX Response codes that are used during File Object Exchange.

212. A POSITA further knows that when a File / Data object is created for OBEX **timestamp is one of the info in the header that is put in an object**. The OBEX transfer disclosure above supports the claim limitations for POSITA about **data object** comprises of new data, data associated and time.

213. Next, Petitioner complains about sending "encrypted data" over the "paired secure Bluetooth connection" for Claim 1 and 6 as purportedly lacking support. I disagree.

214. The specification is clear for the POSITA on the use of data encryption and secure pairing. For example, the specification of the '030 Patent teaches:

[4:09-21] “In order to initiate the **pairing** process, the BT communication device 201 *a* will send the BT communication device name of a predefined number of characters, for example, up to 255 characters, and the BT address to the mobile device 202. The BT communication device 201 *a* then prompts the user of the mobile device 202 to enter the passkey code in order to accept the pairing with the BT communication device 201 *a* on the digital data capture device 201. On entering the passkey by the user of the mobile device 202, the **entered passkey is matched** with the passkey of the BT communication device 201 *a*. If a match is found, a **trusted pair** is automatically established”

[4:20-21] “If a match is found, a trusted pair is automatically established.”

[3:61-64] “A BT device that wants to communicate only with a **trusted device** can **cryptographically** authenticate the identity of another BT device.”

[10:54-56] “The program will use various security, **encryption** and compression **techniques** to enhance the overall user experience.”

215. A POSITA knows that **when passkeys are matched and if a *trusted (secure) pair*** is formed, then Bluetooth cryptographic *link keys* have been exchanged. Link keys are the cryptographic encryption keys. Those same link keys

trusted (secure) pair are used to encrypt/decrypt the data to communicate with the secure *trusted (secure) device*.

216. In my opinion, the disclosures above support the claim limitations about secure trusted pairing, cryptographic, and data encryption.

217. I therefore disagree with Petitioner that any limitation lacks adequate written description support.

B. Validity Analysis of the ‘766 Patent

1. Ground 1 – Singh 129 in View of Singh 906

218. David Lett suggests that a POSITA would have been motivated to combine the teachings of Singh 129 in view of Singh 906 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

219. First, I have examined the scope and content of the cited prior art. With respect to teachings of Singh 129 and Singh 906, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Singh 129 in view of Singh 906 purportedly render the Challenged Claims obvious. I disagree David Lett’s conclusions. Here, I address the most glaring deficiencies in his analysis.

220. In my opinion, there is no reliance on any disclosure from Singh 906 for any Challenged Claim of the ‘766 Patent. In my view, Singh 129 has full written description support for every claim limitation of ‘766 Patent. It is noted that the Examiner did not raise any § 112 objections during prosecution.

221. First, Petitioner has not complained about any Bluetooth, Pairing, Short range, event notification, or polling, claim limitations requiring Singh 906 because all those details are in Singh 129. Indeed, Petitioner states that: “The specification in the priority chain, as shown by **Singh129**, **discloses the first** piece and only the ‘802 application (published as **Singh906**) **discloses the second**.” Petitioner is incorrect because Singh 129, as shown below, discloses the second piece of the limitations.

222. Petitioner further emphasis the need for Singh 906 for the final two claim limitations and states that: “Specifically, it would have been obvious to modify Singh129 in view of Singh906 to provide the **final two** limitations of the independent claims. In the combination, a client application would use HTTP to transfer the new-data along with user information to a user data publishing website over the cellular data network, wherein the user information corresponds to a user identifier that uniquely identifies a particular user of the user data publishing website and is used by the user data publishing website to publish the new-data for private consumption.”

223. Again, there is no need for reliance on Singh 906 for “use HTTP to transfer the new-data along with user information to a user data publishing website over the cellular data network, wherein the user information corresponds to a user identifier that uniquely identifies a particular user of the user data publishing

website and is used by the user data publishing website to publish the new-data for private consumption.”

224. The '030 specification [at 8:43-50] teaches: “The client application 203 automatically **publishes the transferred image** on one or more websites via the internet 501. The user 502 may set **preferences** in the mobile device 202. The user preferences, for example, comprise the web sites selected **for publishing** the transferred image. The user 502 may select websites, for example, Flickr, Picasa, YouTube, eBay(R), etc. and store the preferences on the mobile device 202.”

225. The '030 specification [at 10:04-08] further teaches: “The transport protocol that is used between the **client application 203** and the publishing service 401 may be **hypertext transfer protocol (HTTP)** or extensible markup language-remote procedure calls (XML-RPC).”

226. The '030 specification [at 8:05-08] further teaches: “user publishing information between the client application 203 and the publishing service 401. The user publishing information may, for example, **comprise user preferences** of the websites and the timer setting.”

227. The '030 specification [at 9:21-29] further teaches: “The method and system disclosed herein **enables Jane to** automatically upload pictures and videos taken using her digital camera or video camera onto a mobile device 202 and **publish the pictures**, videos, etc. from her mobile device 202 to the internet 501

with one click or touch of a button. On one click or touch of a button, the pictures and videos are published and immediately made available on **Jane's private blog.**"

228. A POSITA would understand very clearly that the specification text shown above clearly supports the challenged limitations.

229. From a perspective of a POSITA the specific disclosure shown above of "client application", "transport protocol", "HTTP", "**user publishing information**", "**user preferences**", "system disclosed herein **enables Jane to**", "**publish**", "**to Jane private blog**" mean exactly what the last two claim limitations recite.

230. Moreover, as shown below by the Notice of Allowance and Examiner-Initiated interview summary, the claim limitations in the independent claims that Petitioner is complaining about was proposed by the Examiner himself (thus illustrating that he understood what the specifications disclosed). Exhibit 2013 at pages 1 and 9, shown below):

<u>Examiner-Initiated Interview Summary</u>	Application No. 15/640,594	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA Status No

All participants (applicant, applicant's representative, PTO personnel):

(1) SULAIMAN NOORISTANY. (3) ____.

(2) Ashok Tankha Reg. No. 33,802. (4) ____.

Date of Interview: 16 November 2017.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: ____.

Issues Discussed ☐ 101 ☐ 112 ☒ 102 ☐ 103 ☒ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1-20.

Identification of prior art discussed: ____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant agreed that the examiner's amendment, authorized by the above attorney, would place the application in condition for allowance.

Application/Control Number: 15/640,594 Art Unit: 2415	Page 4
--	--------

enabled cellular phone, [[and]] wherein the mobile client application for the
cryptographically authenticated short-range wireless enabled cellular phone is configured
to use HTTP to upload the received new-data along with user information to a user data
publishing website over a cellular data network, and wherein the user information
corresponds to a user identifier that uniquely identifies a particular user of the user data
publishing website and is used by the user data publishing website to publish the new-
data for private consumption.

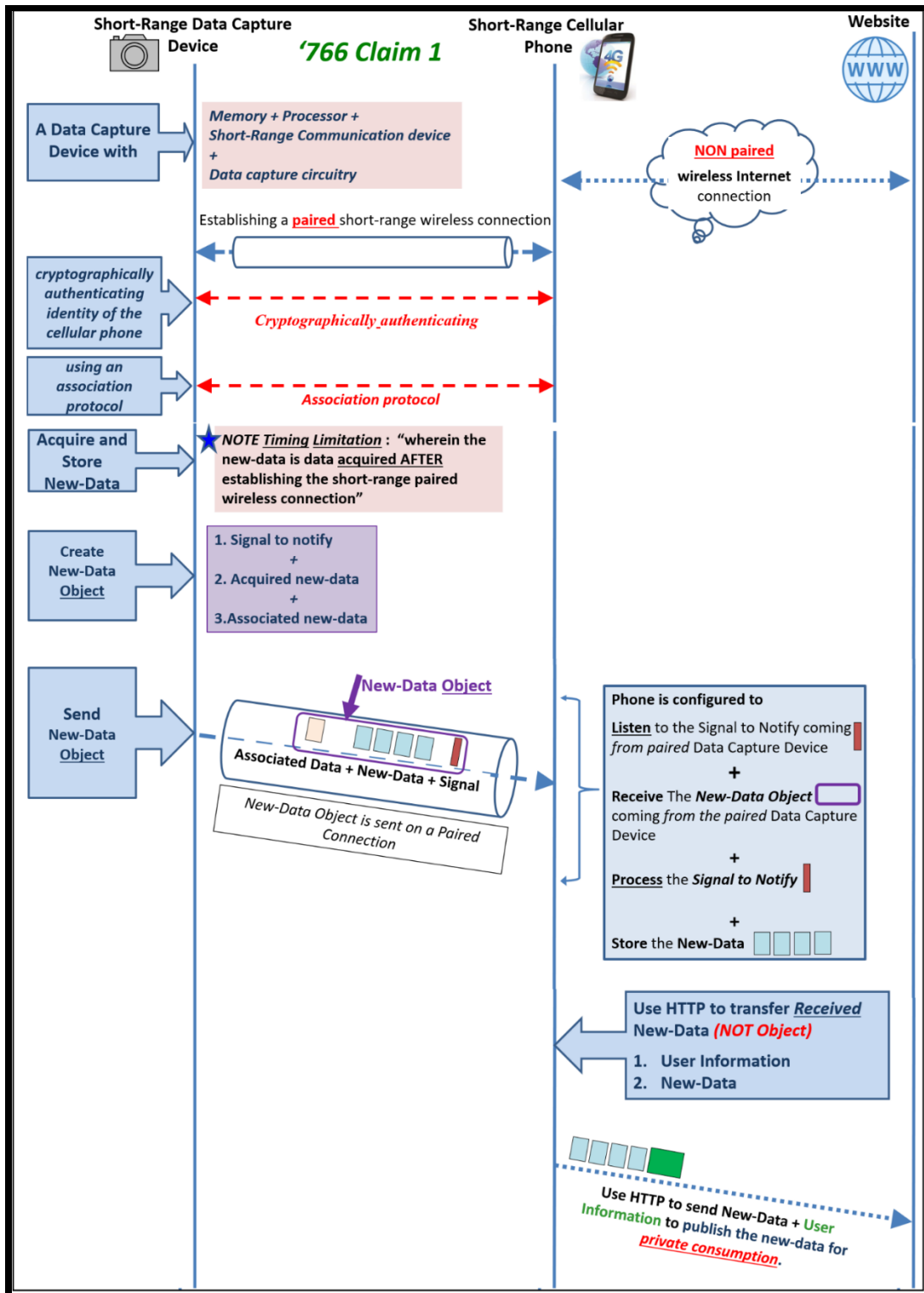
2. Ground 2A – Kahn in View of Bluetooth

231. David Lett suggests that a POSITA would have been motivated to combine the teachings of Kahn in view of Bluetooth in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

232. First, I have examined the scope and content of the cited prior art. With respect to teachings of Kahn and Bluetooth, David Lett provides a claim-by-

claim articulation of his thoughts regarding how the Kahn in view of Bluetooth purportedly render the Challenged Claims obvious. I disagree David Lett's conclusions. Here, I address the most glaring deficiencies in his analysis.

233. As an initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 1 of the '766 Patent as an example):



234. The first glaring deficiency in his analysis is that (as I am informed) the parties have already agreed and adopted the claim construction for the following key terms in the District Court:

“after the paired secure Bluetooth connection is established” /	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device” /
“after establishing a paired Bluetooth connection”	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone”
“after establishing the short-range paired wireless connection” / “after the short-range paired wireless connection is established”	“after the paired connection is established and maintained on a continuous basis between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”

235. Neither Kahn nor Bluetooth disclose a paired connection that is “established and maintained on a continuous basis.”

236. As noted and discussed above, NONE of the prior art (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone paired connection that is “established and maintained on a continuous basis.”

237. In fact, Khan is very clear on NOT maintaining the connection on a continuous basis. According to Khan (at [0058]): “Such an implementation would be appropriate, for example, in cameras that exist **stand-alone (i.e., disconnected)**”

from the host device for significant periods of time.” Khan goes on (at [0079]):
“If the user simply selected to “exit” the dialog, the **applet terminates execution**, as indicated by step 552.” As such, Kahn is NOT maintaining the connection on a continuous basis and Petitioner has not shown otherwise.

238. As for the Bluetooth Core Specification, and as discussed in detail above, Pairing is NOT a default and is only one of the 15 options for connection types. Bluetooth certainly does not teach maintaining that paired connection on a continuous basis. There is NO mention of paired connection which is “established and maintained on a continuous basis” in the Bluetooth Specification.

239. As discussed in detail above, the prior art would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default *for any scenarios*. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

240. As noted and discussed in detail above, in my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification or NOT go with the recommendation

provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

241. In sum, NONE of cited art disclose a paired connection which is **“established and maintained on a continuous basis.”**

242. The second glaring deficiency in the Petition is that “pairing” is not a “must” for a Bluetooth connection (as suggested by the Petitioner and its expert), and both Pairing and Cryptographic Authentication are optional.

243. Petitioner relies **solely** on BT Specification for support for pairing and cryptographically authenticating not on any disclosure in Kahn or Feinberg or Endsely. BUT, in the Bluetooth standard 2.1, the default for bi-directional communication with another Bluetooth device is NOT paired and NOT Authenticated. It is just Encrypted.

244. Upon my review, the words “pair,” “paired,” and “cryptographically authenticating” do NOT appear in any cited art, except the Bluetooth Specification. Once again, I reiterate that the Bluetooth standard makes pairing OPTIONAL. This is because it was NOT done before and not recommended for variety of reasons in 2007 and before.

245. It is my understanding that the construction for both “Paired” and “Cryptographically Authenticating” are agreed by the parties in the District Court:

“paired”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase)”
“short-range paired wireless connection”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase) between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
“cryptographically authenticating”	“verified as legitimate by use of encryption and decryption involving an algorithm”

246. The default 2.1 Bluetooth standard does not require pairing. For example, Bluetooth EDR 2.1 has error codes for when one device attempts to pair with another that does not allow pairing: (1) Pairing Not Allowed (0X18); and (2) Simple Pairing Not Supported (0X37):

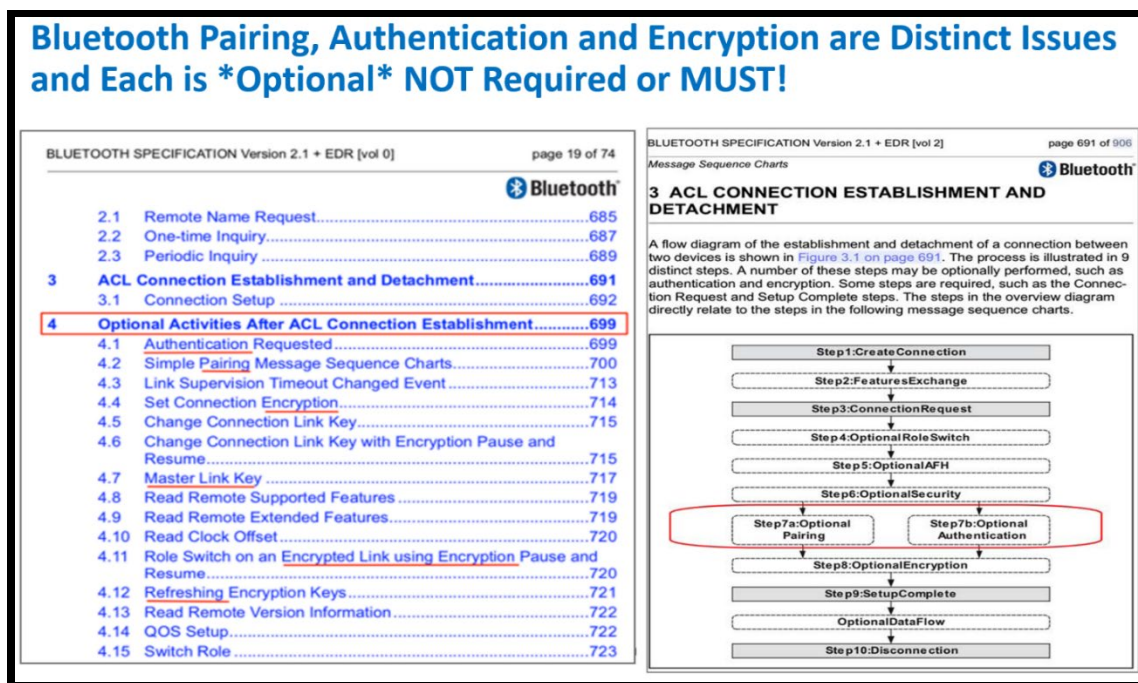
Bluetooth Pairing is Optionally Practiced and Optionally Supported

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0]		page 15 of 74
		Bluetooth
5.2	Parameter Definitions	313
5.3	LMP Encapsulated	323
5.4	Default Values	324
6	List of Figures	325
7	List of Tables	329
Part D ERROR CODES		
Contents		333
1	Overview of Error Codes	335
1.1	Usage Descriptions	335
1.2	HCI Command Errors	335
1.3	List of Error Codes	336
2	Error Code Descriptions	338
2.1	Unknown HCI Command (0X01)	338
2.2	Unknown Connection Identifier (0X02)	338
2.3	Hardware Failure (0X03)	338
2.4	Page Timeout (0X04)	338
2.5	Authentication Failure (0X05)	338
2.6	PIN or key Missing (0X06)	338
2.7	Memory Capacity Exceeded (0X07)	338
2.8	Connection Timeout (0X08)	339
2.9	Connection Limit Exceeded (0X09)	339
2.10	Synchronous Connection Limit to a Device Exceeded (0X0A)	339
2.11	ACL Connection Already Exists (0X0B)	339
2.12	Command Disallowed (0X0C)	339
2.13	Connection Rejected due to Limited Resources (0X0D)	339
2.14	Connection Rejected due to Security Reasons (0X0E)	339
2.15	Connection Rejected due to Unacceptable BD_ADDR (0X0F)	340
2.16	Connection Accept Timeout Exceeded (0X10)	340
2.17	Unsupported Feature or Parameter Value (0X11)	340
2.18	Invalid HCI Command Parameters (0X12)	340
2.19	Remote User Terminated Connection (0X13)	340
2.20	Remote Device Terminated Connection due to Low Resources (0X14)	341
2.21	Remote Device Terminated Connection due to Power Off (0X15)	341
2.22	Connection Terminated by Local Host (0X16)	341
2.23	Repeated Attempts (0X17)	341
2.24	Pairing not Allowed (0X18)	341
2.25	Unknown LMP PDU (0X19)	341
26 July 2007		
BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0]		page 16 of 74
		Bluetooth
2.26	Unsupported Remote Feature / Unsupported LMP Feature (0X1A)	341
2.27	SCO Offset Rejected (0X1B)	341
2.28	SCO Interval Rejected (0X1C)	342
2.29	SCO Air Mode Rejected (0X1D)	342
2.30	Invalid LMP Parameters (0X1E)	342
2.31	Unspecified Error (0X1F)	342
2.32	Unsupported LMP Parameter Value (0X20)	342
2.33	Role Change Not Allowed (0X21)	342
2.34	LMP Response Timeout (0X22)	342
2.35	LMP Error Transaction Collision (0X23)	343
2.36	LMP PDU Not Allowed (0X24)	343
2.37	Encryption Mode Not Acceptable (0X25)	343
2.38	Link Key Can Not be Changed (0X26)	343
2.39	Requested QoS Not Supported (0X27)	343
2.40	Instant Passed (0X28)	343
2.41	Pairing with Unit Key Not Supported (0X29)	343
2.42	Different Transaction Collision (0X2A)	343
2.43	QoS Unacceptable Parameter (0X2C)	343
2.44	QoS Rejected (0X2D)	344
2.45	Channel Classification Not Supported (0X2E)	344
2.46	Insufficient Security (0X2F)	344
2.47	Parameter out of Mandatory Range (0X30)	344
2.48	Role Switch Pending (0X32)	344
2.49	Reserved Slot Violation (0X34)	344
2.50	Role Switch Failed (0X35)	344
2.51	Extended Inquiry Response Too Large (0X36)	344
2.52	Simple Pairing Not Supported By Host (0X37)	345
2.53	Host Busy-Pairing(0X38)	345
Part E HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION		
Contents		349
1	Introduction	357
1.1	Lower Layers of the Bluetooth Software Stack	357
2	Overview of Host Controller Transport Layer	359
3	Overview of Commands and Events	360
3.1	Generic Events	361
3.2	Device Setup	361
3.3	Controller Flow Control	362
3.4	Controller Information	362
26 July 2007		

247. The Bluetooth specification never says pairing is must or is a default requirement for any Bluetooth device. Contrary to Davit Lett and Petitioner’s “must” assertion, the Bluetooth Specification is very clear that Pairing is not required for Bluetooth devices to communicate and Pairing is optional.

248. As noted and discussed in detail above, in Bluetooth “Pairing” is different from “Authentication” and both are different from “Encryption. As shown and discussed above, there are 15 different **optional** activities after a Bluetooth connection is established. Pairing, Authentication, and Encryption are different optional activities. Also, as shown in Figure 3.1 in the v2.1+EDR Bluetooth Core

Specification [Exhibit TTI 1019, p. 861] it again clearly shows that the Pairing is different from Authentication and both of them are different from Encryption.



249. As noted above, there are tens of thousands of possible combinations of optional activities after ACL connection establishment in Bluetooth. Even if all the options are not mutually exclusive, the number of combinations remain a very large number. The Asserted Patents teach one particular combination from the large number of available options. Again, in my opinion, Petitioner is using hindsight reasoning for something which was not a simple design decision in 2007.

250. Moreover, and as noted and discussed in detail above, Petitioner fails to account for the known pairing disadvantages, such as a **poor user experience and battery drain**.

251. Again, and as noted and discussed above, the best way to manage Bluetooth battery usage in 2007 *was to turn off Bluetooth when not in use*: This was the most effective way to conserve battery life as Bluetooth would only drain power when actively searching for or connected to a device.

252. As noted and discussed in detail above, as of 2007, a POSITA would **NOT** be inclined to create a system which required pairing devices because the **Bluetooth specifications didn't require** pairing. Even in 2007, and for Bluetooth 2.1 Security Mode 4, the **default security requirement was an unauthenticated** link key, which doesn't require the entry of a PIN, passkey or comparison of a passkey by the user.

253. Again, and as noted and discussed above, the Bluetooth specification clearly states twice that, “[w]hen both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption.” (Exhibit TTI 1019, p. 1273 and 1286).

254. This statement also means that NOT ALL Bluetooth devices supported pairing. (Conditional statement **when** both device).

255. As noted and discussed above, it would have been these “shall default” Bluetooth options that would have provided for the data security benefits desired by POSITA in 2007. The default connection mode described in the v2.1+EDR Bluetooth core specification is for the connection to be *unpaired*,

encrypted, unauthenticated and unauthorize. Exhibit TTI 1019, p. 1273 and 1286.

Without some other specific requirement in place for a connection to be paired, there is no reason that a POSITA would not choose the default connection (unencrypted, authenticated and/or authorized).

256. In 2007 a POSITA understood that the Basic Imaging Profile (BIP) describes all the Kahn, Hiroishi, Feinberg, Endsley scenarios. However, BIP did not require a paired Bluetooth connection for all these scenarios. For the scenarios most in line with Kahn, Hiroishi, Feinberg, Endsley, *i.e.* pull based or push based mage transfer, BIP was not recommending using a paired Bluetooth connection.

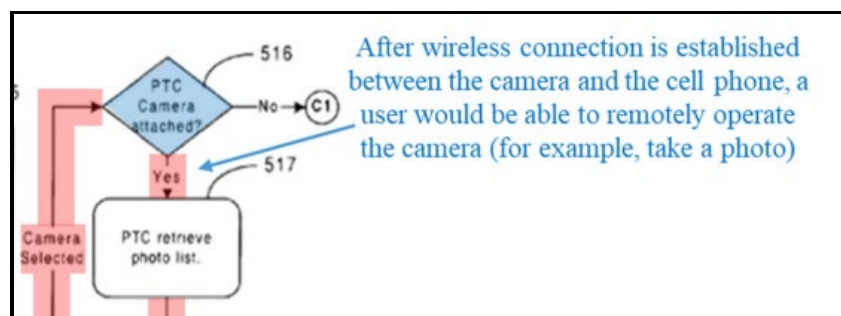
257. NONE of the cited references (Kahn, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default *for any scenarios*. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

258. As discussed in detail above, in my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to

Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification or NOT go with the recommendation provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

259. The third glaring deficiency in Petitioner’s analysis is that *timing of acquiring new data is NOT after pairing*.

260. For the timing of acquiring new data “after” pairing limitation, Petitioner relies on Kahn as follows: “Figure **5B** of Kahn contemplates a control loop where new pictures are acquired after a connection has been established.”

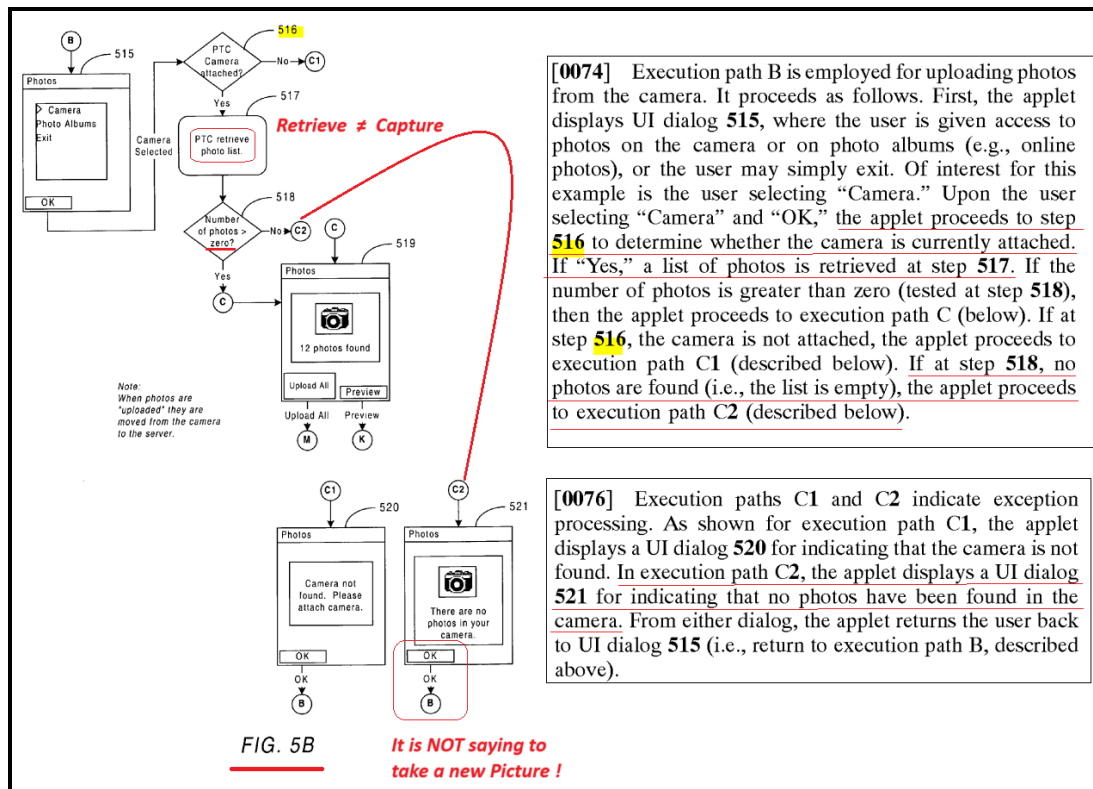


261. There is nothing in Kahn that actually does any capturing of the images *after* connection is established. In fact, what the Kahn Figure **5B** and the text describing the Figure **5B** flow chart section (516 and 517 element) says is the complete opposite, as illustrated below:

Kahn [0074]: “Upon the user Selecting “Camera’ and “OK, the applet proceeds to **Step 516** to determine whether the camera is **currently attached**. If “Yes,” a list of photos is **retrieved** at step 517.”

Kahn [0074]: “**If** at step 518, **no photos** are found (i.e., the list is empty), the applet proceeds to execution path **C2** (described below).”

Kahn [0076]: “In execution path **C2**, the applet displays a **UI dialog** 521 for **indicating** that **no photos** have been found in the camera.”



262. ALL of the Challenged Claims expressly require *Acquire or Capture after pairing connection*. In Kahn, there is NO capturing of the photos after the connection is established in Fig 5B or the accompanying text for **Fig 5B**. Element (517) “Retrieve photo list” is to get photos that **already exist** is not same as “capture a new photo”. There is no mention of capturing a new photo after the PTC camera is attached. **Retrieve ≠ Capture** and **Retrieve ≠ Acquire**.

263. As understood by a POSITA, “Retrieval” means to access or bring back something that is *already stored*, like recalling information from memory. while “acquire” means to gain or obtain *something new*, like learning a skill or getting a possession; essentially, retrieval is about accessing existing information,

while acquiring is about getting something you didn't have before. Acquire/Capture is the initial step of gathering data.

264. The **Fig 5B** work flow in Kahn is even more clear about NOT acquiring the new data after connection. There is NO mention of acquiring or capturing new photos. The state machine is about “retrieval” and “upload”. In the Fig 5B state machine even when there are ZERO photos to upload state machine goes to C2. And “C2” GUI does not require the taking of a new picture.

265. In fact, Kahn is teaching the opposite, as illustrated at Khan [0097]: “The method steps are as follows. As indicated at **Step 701**, one or more images are **captured**/recorded at the camera device. Next, at **Step 702**, the images are associated with the user's location (i.e., location ID, based on GPS information). Typically, this occurs when the **camera is attached to the local host**. Upon attachment of the camera to the local host, the images are either automatically uploaded or the user manually requests uploading.”

266. It clearly says in Kahn [0097] that “capture image” happens first, **and then attach** to the local host for uploading.

267. Kahn also says (in [0058]): “Such an **implementation would be appropriate**, for example, in **cameras** that exist stand-alone (*i.e.*, **disconnected**) from the host device for **significant** periods of time.”

268. Again, Kahn is teaching the complete opposite of what the Challenged Claims recite. The reason for that opposite teaching is because for a POSITA in 2004 you connected only when you needed to upload and then disconnected to save the precious little battery life on the phone.

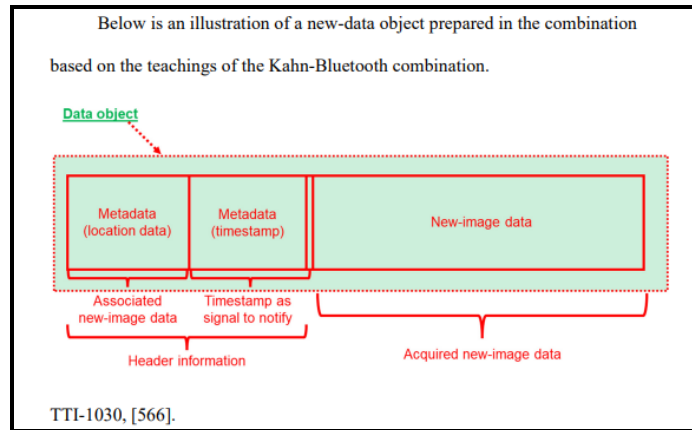
269. The fourth glaring deficiency: “Object” is not the same as “File.”

270. As discussed in detail above, a POSITA would understand the fact that an “object” is not the same as a “file” (as discussed in the claim construction portion, above). As such, the Petition fails to disclose any prior art meeting this limitation, as no art shows a creation of an “Object.” As discussed in detail above, the “timestamp” of a file cannot be viewed as being the claimed “signal to notify.”

271. Again, a Signal to Notify inside an Object cannot be the same as a “Timestamp” in a File about the time it was created. That would mean for every protocol that transfers a file on the internet, the receiving endpoint is checking the (creation) timestamp in the received file and processing it as a “signal to notify.”

272. The fifth glaring deficiency is that the Kahn **“file timestamp” sent in an (file) object cannot** be considered a “signal to notify” for new data.

273. Petitioner asserts that Time stamp in Kahn is considered a signal to notify in the data object:



274. In Kahn, the “file timestamp” sent in an (file) object cannot be considered a “signal to notify” **because signal to notify for the new-data has to be the first time the cellphone becomes aware of that there is new data on the camera. It cannot be the second or third message from the camera about the data/photo being created on the camera.**

275. Returning to the language of the Challenged Claims:

“said processor further configured to **create a new-data object**, wherein the new-data object comprises:

signal to notify, wherein the **signal to notify corresponds to the acquiring of the new-data for transfer** to the cryptographically authenticated short-range wireless enabled cellular phone;

the acquired new-data; and

associated new-data, wherein the associated new-data corresponds to data associated with the new-data; and

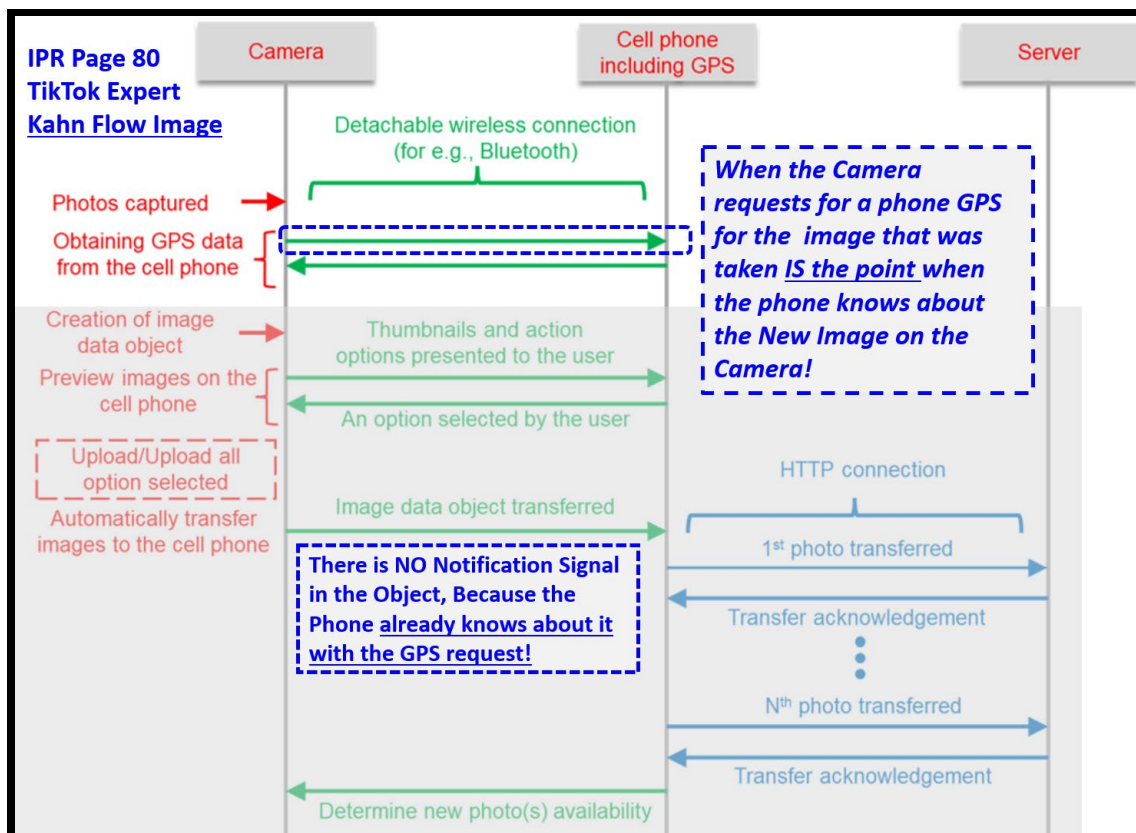
said processor further configured to **transfer automatically the new-data object to** the cryptographically authenticated short-range wireless enabled **cellular phone**, over the established short-range paired wireless connection, wherein the cryptographically authenticated short-range wireless enabled **cellular phone is configured to listen to the signal to notify** and receive the new-data object over the established short-range paired wireless connection, wherein a **mobile client application** for the cryptographically authenticated short-range wireless enabled cellular phone is configured to **process the signal to notify**”

276. Summarizing the claims at issue: the claim requires “create a new-data object,” that has “signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer,” then “transfer automatically the new-data object to” “cellular phone,” where the “cellular phone is configured to listen to the signal to notify” and the “mobile client application “process the signal to notify.”

277. The claim requires that the first time the phone received the new data object, that is the first time the phone knows/or becomes aware of this new data, because the signal to notify is embedded inside the new data Object. And the phone has NOT been aware of the existence of this data/photo before the phone received this signal to notify for the new data.

278. A POSITA would understand and appreciate the fact that if the Phone already knows about this photo (new data) existing before he gets the object, then it is not a signal to notify for new-data/photo. It is more of a message of the data the phone already knows that it exists.

279. In Khan's state machine (as illustrated and annotated below), the **first time** the phone is made aware of the existence of the new photo is when the camera makes a request to the cellphone for the GPS location, using the location API. If anything, this first request for location GPS to the phone by the camera is the FIRST "signal to notify" to the phone by the camera about the existence of the new photo on the camera:



280. The first indication to the phone about the existence of the photo is NOT when the phone received the image file (GPS + timestamp + image) as one unit, that was created using the GPS information sent from the phone.

281. When the phone receives the image file (GPS + timestamp + image), the phone already knows about the existence of the new photo **beforehand, by virtue of having received the request for GPS information** for the said photo, prior to receiving the image file.

282. The fact that phone knows that this photo existed before the image file comes, makes the timestamp in the image “not a signal to notify” for new data captured by the camera.

283. Moreover, for the “*listening to the signal to notify*” limitation, Petitioner asserts that “which constitutes as listening to the signal to notify. TTI-1017, [0057]; see also id., [0074], [0076], FIG. 5B.”

284. BUT a review of Kahn TTI-1017, [0057]; [0074], [0076] and FIG. 5B shows **NO “listening” by the Kahn phone or applet for ANY kind of “timestamp”** (*i.e.*, the alleged signal to notify). In fact, the word “listen” or “listening” is NOWHERE in the whole of Kahn.

285. **There is NO “Processing” by the Kahn phone or applet for ANY kind of “timestamp”** inside the transferred file, the alleged signal to notify according to petitioner’s assertion. Petitioner seeks to rely on Khan [0071] and

[0055] for processing support, but this is not sufficient. In fact, NOWHERE in the whole Kahn disclosure does it show Kahn *applet processing timestamps inside* the received file from the camera.

286. Kahn does NOT support the whole limitation at issue [1.10] – [1.16] about: creating, sending, listening, and processing signal to notify *i.e.* timestamp inside the file. Petitioner apparently recognizes this, as well, which is the basis for the asserted *Feinberg* combination.

287. The fifth glaring deficiency in Petitioner’s analysis is that Kahn does NOT teach use of HTTP for uploading photos/media. Instead, it required using WMTP for media upload. As discussed at length and in detail above, HTTP and WMTP are clearly NOT interchangeable.

288. As discussed in detail above, as of 2004, WAP and WMTP were the wireless communication technique, and HTTP were the *standard protocol for the web*. As such, when Kahn says the upload process “occurs via wireless communication technique,” he means wireless WAP and wireless WMTP protocols (NOT HTTP). Indeed, and as discussed above, Kahn clearly teaches the *exclusive use of WMTP*.

289. Further, and as discussed in detail above, Kahn makes it clear that WMTP is exclusively used for uploading. The result is that Kahn clearly informs

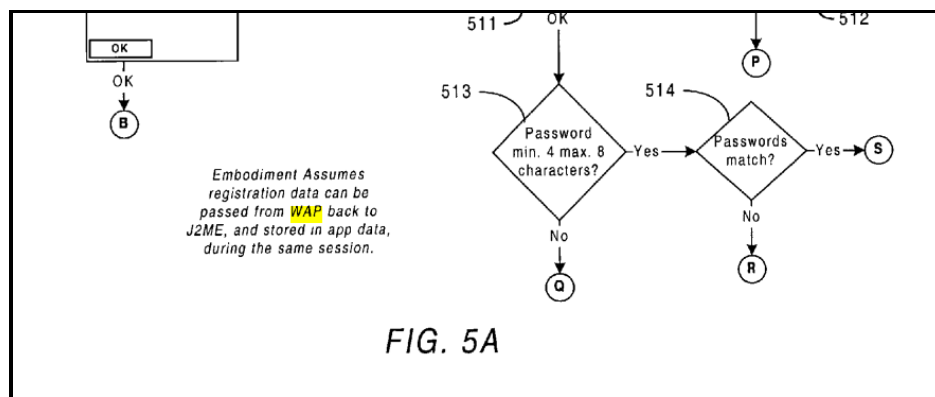
the POSITA to use WMTP (which is a wireless protocol, whereas HTTP is and was a web protocol).

290. As discussed in detail above, Kahn Fig. 5D, element 543, mentions WAP, which was being pushed in the industry at the time (with WMTP). These protocols were specifically designed for mobile devices with limited bandwidth, with WAP acting as a gateway to translate requests from a mobile phone into standard HTTP requests, whereas HTTP (Hypertext Transfer Protocol) is the standard protocol used for web browsing on traditional computers. WMTP and WAP were particularly relevant in the early days of mobile internet when data capabilities were significantly lower. Thus, when Kahn references “wireless communication techniques” in [0057] for “uploading,” it very clearly shows two wireless protocols WMTP and WAP in Fig 5D. It is thus clear that Kahn wants to use wireless protocols like WMTP for upload and NOT web protocol HTTP.

291. As discussed in detail above, Kahn assumes the POSITA knows about WAP architecture and usage in the wireless domain. Just like a POSITA for the wired network would know about TCP/IP or OSI stack, Kahn assumes the POSITA is knowledgeable about the WAP architecture and WMTP in the WAP system. Indeed, Kahn talks about wireless transmission techniques and in the detailed diagrams it mentions WMTP and WAP.

292. As noted and discussed in detail above, a WAP architecture system, the “wireless modular transport protocol” (WMTTP) refers to the Wireless Datagram Protocol (WDP), which acts as the transport layer within the WAP stack, providing a flexible way to transfer data across different network types, even when dealing with unreliable or limited bandwidth connections typical in mobile networks; essentially acting as a modular adaptation layer for various underlying bearer services. As discussed in detail above, it is clear that Kahn intends for the POSITA to use WAP architecture and system. *See* Khan at [0017].

293. Once again, as discussed above, WAP is also described in Kahn **Fig 5A**, it is clear that in Kahn 5A, WAP is used to connect the mobile app (J2ME Applet in 2004) to the outside internet for login registration and password. It is NOT HTTP, but WAP that is used for login password and registration.



294. Still further, and as discussed in detail above, as of 2004, WAP was considered better than HTTP for mobile devices for a variety of reasons, including:

(i) optimized for mobile devices; (ii) efficient use of bandwidth; (iii) security; and (iv) adaptation to wireless networks.

295. As further discussed in detail above, to the extent Kahn discussed HTTP, it does so in the context of ecommerce only – not for uploading photos. In addition, Kahn teaches the use of HTTP to obtain GPS data via a location API call. Such is not going out to the server.

296. To reiterate what is discussed in detail above, Kahn is very clear to the POSITA on what protocols to use and where. Specifically: HTTP for e-commerce and internal hardware chip location API. As for uploading/media-transfer and login information, on the other hand, Kahn is very clear to POSITA to use WMTP.

297. As discussed above, Petitioner's assertion that POSITA would use HTTP instead of the clear teaching of WMTP in Kahn for uploading/media-transfer/login is not supported at all in Kahn, and does not reflect the approach to be taken by a POSITA.

298. Moreover, and as discussed in detail above, a POSITA would readily appreciate the fact that WMTP and HTTP are very different protocols and they are NOT Interchangeable. Indeed, WMTP and HTTP run on different layers of the OSI stack, and there are numerous other significant differences between these two protocols (as discussed above).

3. Ground 2B – Kahn in View of Feinberg and Bluetooth

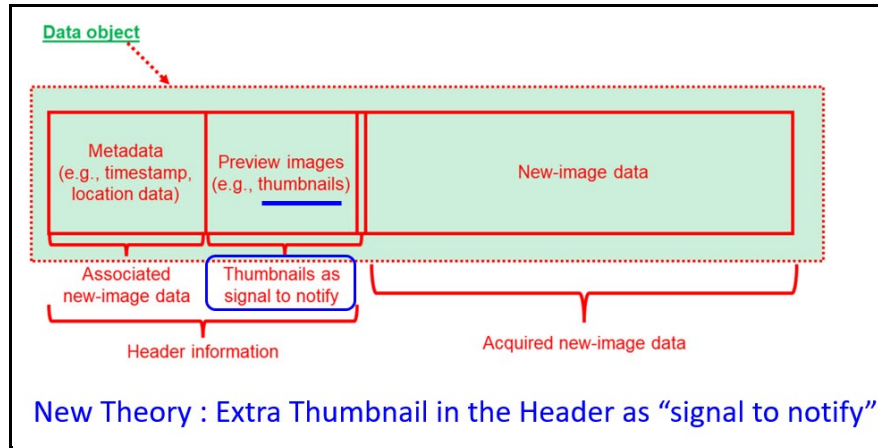
299. David Lett suggests that a POSITA would have been motivated to combine the teachings of Kahn in view of Feinberg and Bluetooth in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

300. First, I have examined the scope and content of the cited prior art. With respect to teachings of Kahn and Feinberg and Bluetooth, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Kahn in view of Feinberg and Bluetooth purportedly render the Challenged Claims obvious. I disagree David Lett's conclusions. Here, I address the most glaring deficiencies in his analysis.

301. Petitioner apparently realizes the fact that Kahn does not disclose the claimed "signal to notify," so it proceeds to suggest an alternative combination further including Feinberg. Of course, Feinberg does not disclose the transfer of thumbnails to the mobile phone, inasmuch as it prefers the use of a media card on the camera, which communicates with a Home Network Access Point, which, in turn, communicates with a third-party website.

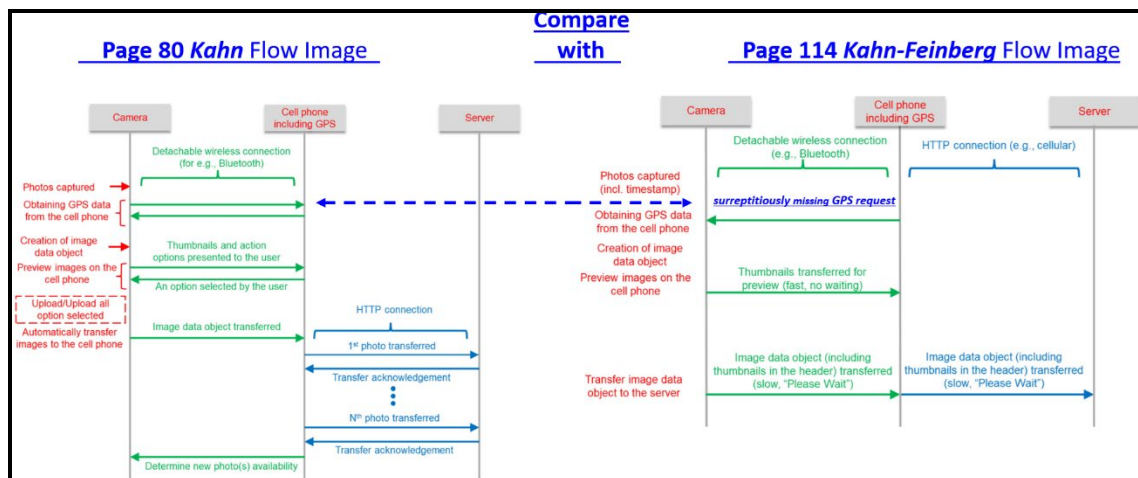
302. The Petitioner is clear that it relies on Feinberg for signal to *notify*; Petitioner expressly states: "Accordingly, the entirety of the analysis in Ground 2A applies to Ground 2B, **with the exception that the signal to notify in this Ground is provided by the thumbnails** in the header of the data object."

303. Petitioner wants to add an extra thumbnail in the file using Feinberg and wants to assume that this extra thumbnail in the file is the “signal to notify” for Ground 2B. An annotated version of Petitioner’s image in its Petition is set forth below:



304. First, neither Feinberg nor Kahn teaches creating an Object, therefore the combination cannot be teaching an Object either. *Even if we were to assume a new “file” with a thumbnail in the header is an object* the combination (which it is not) the **combination still fails**.

305. Petitioner shows the new flow diagram that has added thumbnails. But on inspection, it is missing one key piece. Specifically, Petitioner *surreptitiously removed the GPS request coming from the camera to the phone*. Petitioner’s images from its Petition are shown below side by side for comparison:



306. As shown, Petitioner and its expert have removed the Request from the Camera to the Phone for the GPS. In Kahn, however, it is the camera that **first** sends a request to the phone for GPS information for the image that was just taken. *When the phone receives this request for GPS information, it is at this point when the phone knows about the New Image on the Camera.* NO signal to notify is required after that, about the new data, because the phone now already knows the existence of new data.

307. Petitioner's image is clearly incomplete, because without the request from the camera, how and why is the phone responding to with GPS information in the second diagram, and what is the trigger for the phone for sending the GPS information to the camera in the new flow?

308. The Feinberg combination fails for the same reason the combination failed for just Kahn. In Khan's state machine, and as discussed above, the first time the phone is made aware of the existence of the new photo is when the camera

makes a request to the cellphone for the GPS location, using the location API. If anything, this first request for location GPS to the phone by the camera is the FIRST “signal to notify” to the phone by the camera about the existence of the new photo on the camera.

309. Summarizing the Challenged Claim: the claim requires “create a new-data object,” that has “signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer,” then “transfer automatically the new-data object to” a “cellular phone,” which “is configured to listen to the signal to notify,” and “mobile client application “process the signal to notify.”

310. The claim requires that the first time the phone receives the new data object, that is the first time the phone knows/or becomes aware of this new data, because the signal to notify is embedded inside the new data Object. And the phone has NOT been aware of the existence of this data/photo before the phone received this signal to notify for the new data.

311. If the Phone already knows about this photo (new data) existing before he gets the object, then it is not a signal to notify for new-data/photo. It is more of a message of the data the phone already knows that it exists.

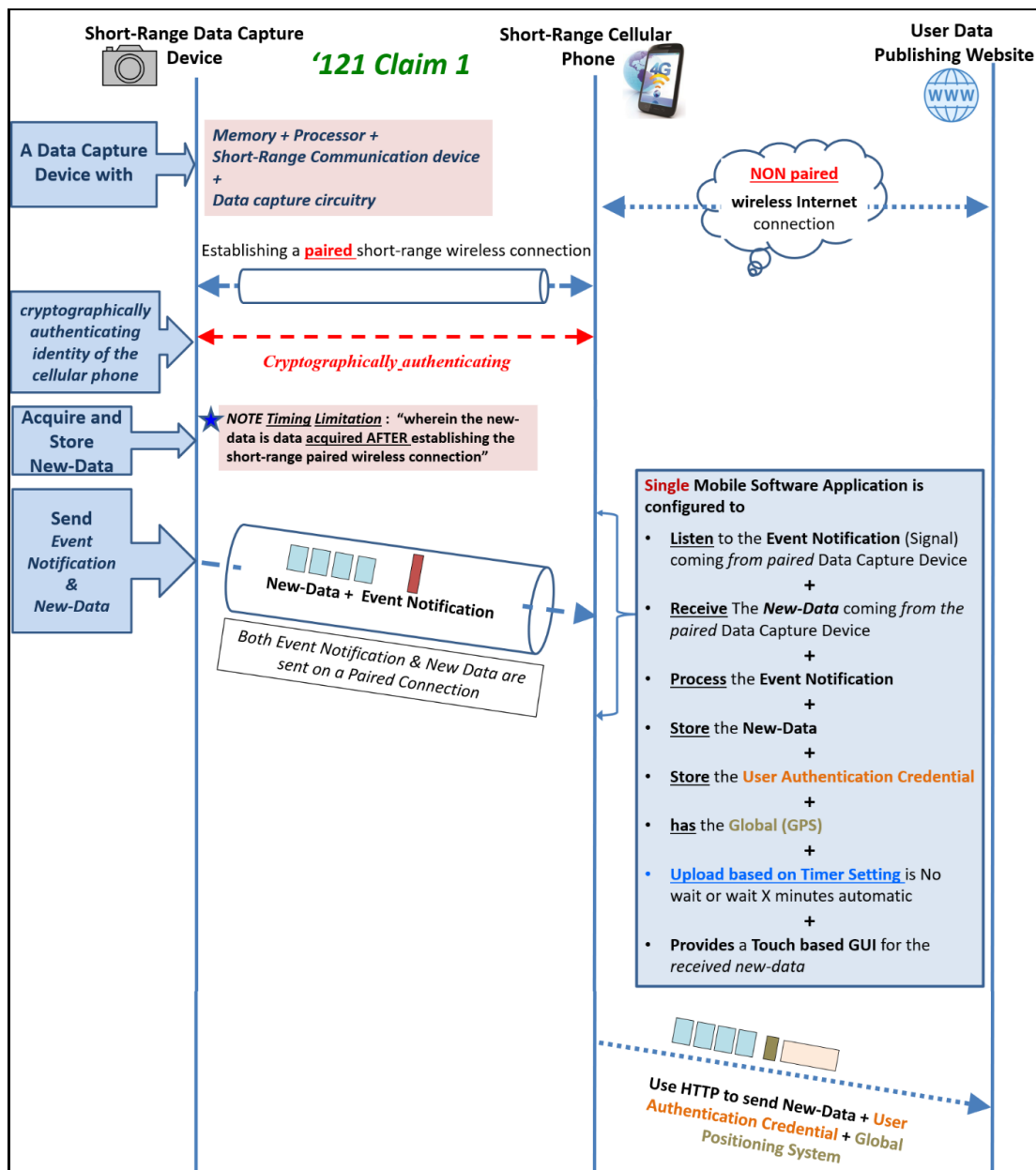
C. Validity Analysis of the ‘121 Patent

1. Ground 1 – Hiroishi in view of Kahn, Endsley, and Bluetooth

312. David Lett suggests that a POSITA would have been motivated to combine the teachings of Hiroishi in view of Kahn, Endsley, and Bluetooth in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

313. First, I have examined the scope and content of the cited prior art. With respect to teachings of Hiroishi, Kahn, Endsley, and Bluetooth, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Hiroishi in view of Kahn, Endsley, and Bluetooth purportedly render the Challenged Claims obvious. I disagree David Lett’s conclusions. Here, I address the most glaring deficiencies in his analysis.

314. As an initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 1 of the ‘121 Patent as an example):



315. The First glaring deficiency in Petitioner's analysis is that (as discussed above) both parties have already agreed and adopted the claim construction for key terms including:

"after the paired secure Bluetooth connection is established" /

"after the paired connection **is established and maintained on a continuous basis** between the Bluetooth enabled data capture device and the

“after establishing a paired Bluetooth connection” “after establishing the short-range paired wireless connection” / “after the short-range paired wireless connection is established”	Bluetooth enabled mobile device” / “after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone” “after the paired connection is established and maintained on a continuous basis between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”
---	---

316. Neither Hiroshi, Kahn, Endsley, or Bluetooth disclose a paired connection that is “established and maintained on a continuous basis,” and Petitioner has not made any contrary showing.

317. Again, NONE of the prior art (Kahn, Hiroishi, Feinberg, Endsley) even mentions the word “pair” or “pairing,.” Let alone a paired connection which is “established and maintained on a continuous basis.”

318. As discussed in detail above, as of 2007 a POSITA would NOT “maintain a paired connection on a continuous basis,” which is required under the agreed claim construction from the District Court.

319. The second glaring deficiency in Petitioner’s analysis is that “pairing” is not a “must” for a Bluetooth connection, and both Pairing and Cryptographic Authentication are Non-Obvious.

320. I understand that in the Institution decision for the ‘121 Patent (at 42), the Board stated that: “Petitioner, for example, has demonstrated a reasonable likelihood of prevailing in showing that the connection between Hiroishi’s camera and mobile *phone is “paired,” given that there is bidirectional communication* between the devices through Bluetooth, and that cryptographic authentication as claimed is part of the Bluetooth pairing process.”

321. Of course, a POSITA would appreciate that two Bluetooth devices can have bi-directional communication between them **without ever pairing** (even today). In fact, and as discussed in detail above, in the Bluetooth standard 2.1, the default for bi-directional communication with another Bluetooth device is NOT paired and NOT Authenticated. It is just Encrypted.

322. As discussed in detail above, I understand that “Paired” and “Cryptographically Authenticating” are terms that have been agreed to by the parties in the District Court, as follows:

“paired”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase)”
“short-range paired wireless connection”	“in the condition of having an exchanged link key (either before connection establishment was requested or during connecting phase) between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”

“cryptographically authenticating”	“verified as legitimate by use of encryption and decryption involving an algorithm”
------------------------------------	---

323. The totality of Petitioner’s assertion for “paired” connection is set forth below. There is no analysis or explanation as to **why** Hiroishi’s camera’s short-range wireless communication device is configured to establish a short range paired wireless connection. In fact, the Hiroishi disclosure has NO mention of pair, or pairing, and NOT all Bluetooth devices support optional pairing.

[1.3.1]

Hiroishi-Kahn-Endsley-Bluetooth renders obvious [1.3.1]. TTI-1030, [923].

In the combination, Hiroishi’s camera includes a short-range wireless communication device (“communication unit 59”) configured to establish a short-range paired wireless connection (a Bluetooth connection) between the short-range wireless enabled data capture device (camera 50) and a short-range wireless enabled cellular phone (“mobile phone 40”). TTI-1011, FIG. 1-3, [0043]-[0049], [0051]-[0052], [0058], [0066]-[0067], FIG. 4 (reproduced below); TTI-1019, 87.

33

324. As noted and discussed in detail above, the default 2.1 Bluetooth standard does not require pairing. For example, Bluetooth EDR 2.1 has error codes for when one device attempts to pair with another that does not allow pairing: (1) Pairing Not Allowed (0X18); and (2) Simple Pairing Not Supported (0X37).

325. I note that Petitioner cites to: Davit Lett, expert report TTI-1030 page 923. I do not find the existence of any such page 923. In any event, the Hiroshi

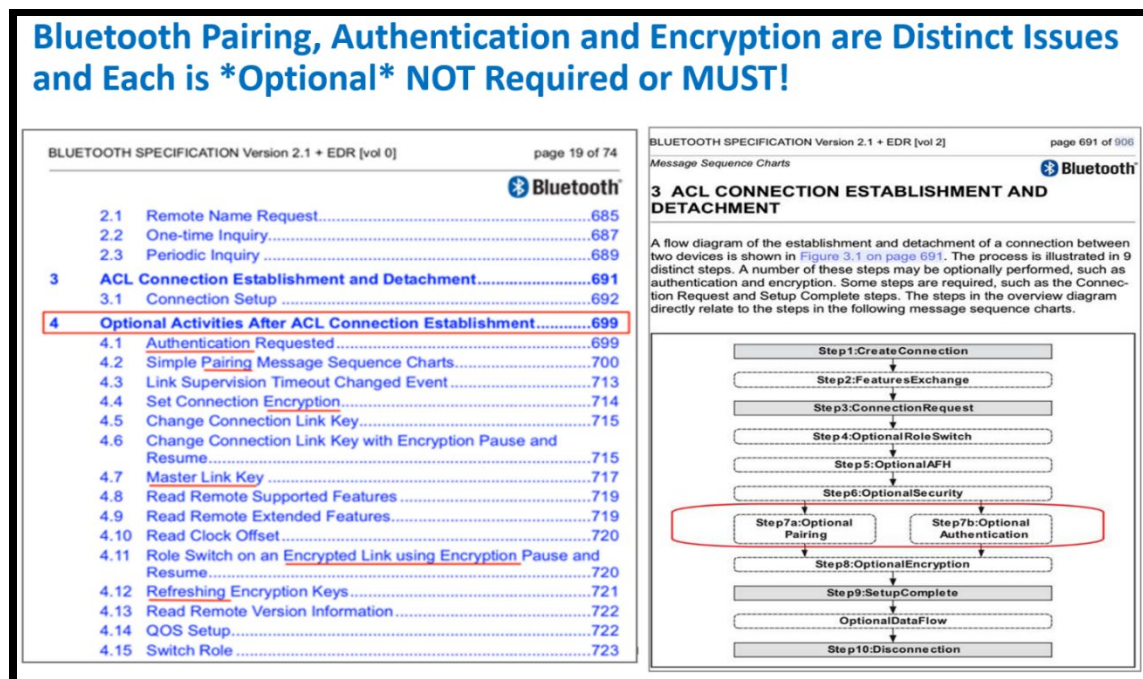
disclosure has ZERO mention of “pair” or “pairing”. It also has no mention of “link key” exchanging link keys, anywhere in the whole document. Likewise, the TTI-1019 Bluetooth specification page 87 has NO Mention of pair or pairing on that page.

Bluetooth Pairing is Optionally Practiced and Optionally Supported	
BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0] page 15 of 74 Bluetooth 5.2 Parameter Definitions 313 5.3 LMP Encapsulated 323 5.4 Default Values 324 6 List of Figures 325 7 List of Tables 329 Part D ERROR CODES Contents 333 1 Overview of Error Codes 335 1.1 Usage Descriptions 335 1.2 HCI Command Errors 335 1.3 List of Error Codes 336 2 Error Code Descriptions 338 2.1 Unknown HCI Command (0X01) 338 2.2 Unknown Connection Identifier (0X02) 338 2.3 Hardware Failure (0X03) 338 2.4 Page Timeout (0X04) 338 2.5 Authentication Failure (0X05) 338 2.6 PIN or key Missing (0X06) 338 2.7 Memory Capacity Exceeded (0X07) 338 2.8 Connection Timeout (0X08) 339 2.9 Connection Limit Exceeded (0X09) 339 2.10 Synchronous Connection Limit to a Device Exceeded (0X0A) 339 2.11 ACL Connection Already Exists (0X0B) 339 2.12 Command Disallowed (0X0C) 339 2.13 Connection Rejected due to Limited Resources (0X0D) 339 2.14 Connection Rejected due to Security Reasons (0X0E) 339 2.15 Connection Rejected due to Unacceptable BD_ADDR (0X0F) 340 2.16 Connection Accept Timeout Exceeded (0X10) 340 2.17 Unsupported Feature or Parameter Value (0X11) 340 2.18 Invalid HCI Command Parameters (0X12) 340 2.19 Remote User Terminated Connection (0X13) 340 2.20 Remote Device Terminated Connection due to Low Resources (0X14) 341 2.21 Remote Device Terminated Connection due to Power Off (0X15) 341 2.22 Connection Terminated by Local Host (0X16) 341 2.23 Repeated Attempts (0X17) 341 2.24 Pairing not Allowed (0X18) 341 2.25 Unknown LMP PDU (0X19) 341 26 July 2007	BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0] page 16 of 74 Bluetooth 2.26 Unsupported Remote Feature / Unsupported LMP Feature (0X1A) 341 2.27 SCO Offset Rejected (0X1B) 341 2.28 SCO Interval Rejected (0X1C) 342 2.29 SCO Air Mode Rejected (0X1D) 342 2.30 Invalid LMP Parameters (0X1E) 342 2.31 Unspecified Error (0X1F) 342 2.32 Unsupported LMP Parameter Value (0X20) 342 2.33 Role Change Not Allowed (0X21) 342 2.34 LMP Response Timeout (0X22) 342 2.35 LMP Error Transaction Collision (0X23) 343 2.36 LMP PDU Not Allowed (0X24) 343 2.37 Encryption Mode Not Acceptable (0X25) 343 2.38 Link Key Can Not be Changed (0X26) 343 2.39 Requested QoS Not Supported (0X27) 343 2.40 Instant Passed (0X28) 343 2.41 Pairing with Unit Key Not Supported (0X29) 343 2.42 Different Transaction Collision (0X2A) 343 2.43 QoS Unacceptable Parameter (0X2C) 343 2.44 QoS Rejected (0X2D) 344 2.45 Channel Classification Not Supported (0X2E) 344 2.46 Insufficient Security (0X2F) 344 2.47 Parameter out of Mandatory Range (0X30) 344 2.48 Role Switch Pending (0X32) 344 2.49 Reserved Slot Violation (0X34) 344 2.50 Role Switch Failed (0X35) 344 2.51 Extended Inquiry Response Too Large (0X36) 344 2.52 Simple Pairing Not Supported By Host (0X37) 345 2.53 Host Busy-Pairing(0X38) 345 Part E HOST CONTROLLER INTERFACE FUNCTIONAL SPECIFICATION Contents 349 1 Introduction 357 1.1 Lower Layers of the Bluetooth Software Stack 357 2 Overview of Host Controller Transport Layer 359 3 Overview of Commands and Events 360 3.1 Generic Events 361 3.2 Device Setup 361 3.3 Controller Flow Control 362 3.4 Controller Information 362 26 July 2007

326. Petitioner asserts that the Hiroshi camera short range communication device must be configured to pair. This is without any factual support, and the fact is that Bluetooth never says pairing is must or is a default requirement for any Bluetooth device. Contrary to Petitioner’s assertions, the Bluetooth Specification is

very clear that Pairing is not required for Bluetooth devices to communicate and Pairing is optional.

327. As noted and discussed in detail above, in Bluetooth “Pairing” is different from “Authentication” and both are different from “Encryption. As shown and discussed above, there are 15 different **optional** activities after a Bluetooth connection is established. Pairing, Authentication, and Encryption are different optional activities. Also, as shown in Figure 3.1 in the v2.1+EDR Bluetooth Core Specification [Exhibit TTI 1019, p. 861] it again clearly shows that the Pairing is different from Authentication and both of them are different from Encryption.



328. For a POSITA, these options are chosen for a connection depending on the requirements of the solution being implemented. In the Bluetooth family of

specifications, Profile specifications are used to describe how to implement a particular use case or family of related use cases. POSITA would listen to recommendations from the v2.1+EDR Bluetooth Core specification or the Bluetooth Basic Imaging Profile (BIP) specification.

329. As noted above, there are tens of thousands of possible combinations of optional activities after ACL connection establishment in Bluetooth. Even if all the options are not mutually exclusive, the number of combinations remain a very large number. The Asserted Patents teach one particular combination from the large number of available options. Again, in my opinion, Petitioner is using hindsight reasoning for something which was not a simple design decision in 2007.

330. Moreover, and as noted and discussed in detail above, Petitioner fails to account for the known pairing disadvantages, such as a **poor user experience and battery drain**.

331. Again, and as noted and discussed above, the best way to manage Bluetooth battery usage in 2007 *was to turn off Bluetooth when not in use*: This was the most effective way to conserve battery life as Bluetooth would only drain power when actively searching for or connected to a device.

332. As noted and discussed in detail above, as of 2007, a POSITA would **NOT** be inclined to create a system which required pairing devices because the **Bluetooth specifications didn't require** pairing. Even in 2007, and for Bluetooth

2.1 Security Mode 4, the **default security requirement was an unauthenticated** link key, which doesn't require the entry of a PIN, passkey or comparison of a passkey by the user.

333. Moreover, **Hiroshi [0067] teaches one to follow the Bluetooth Standards:** "Therefore, the communication unit 49 of the mobile phone 40 and the communication unit 59 of the digital camera 50 are configured so as to allow a communication **according to the standard of Bluetooth**, respectively." For Petitioner to suggest otherwise is contrary to Hiroshi's teaching.

334. Again, and as noted and discussed above, the Bluetooth specification clearly states twice that, "[w]hen both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption." (Exhibit TTI 1019, p. 1273 and 1286).

335. This statement also means that NOT ALL Bluetooth devices supported pairing. (Conditional statement **when** both device).

336. As noted and discussed above, it would have been these "shall default" Bluetooth options that would have provided for the data security benefits desired by POSITA in 2007. The default connection mode described in the v2.1+EDR Bluetooth core specification is for the connection to be *unpaired, encrypted, unauthenticated and unauthorize*. Exhibit TTI 1019, p. 1273 and 1286. Without some other specific requirement in place for a connection to be paired,

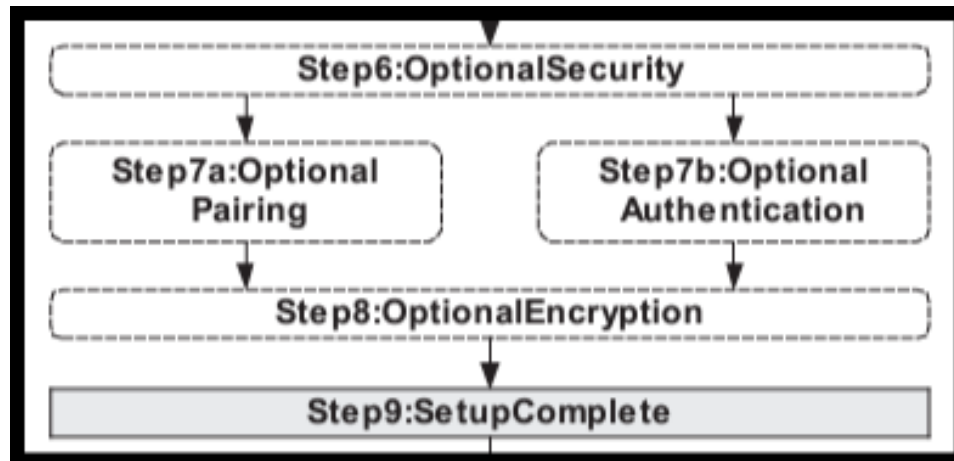
there is no reason that a POSITA would not choose the default connection (unencrypted, authenticated and/or authorized).

337. As discussed above, NONE of the cited references (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default for any scenarios. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

338. I note that NONE of the cited references (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default *for any scenarios*. Data Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

339. Petitioner wrongly asserts that “cryptographically authenticating the identity of phone 40 was a required to pair Hiroishi’s Bluetooth camera 50 and

phone 40.” Again, this statement is offered without any factual support, and which is incorrect. One can have a paired connection without being authenticated, and one can have a authenticated connection without being paired.



340. Hiroshi does not disclose the “Cryptographically Authenticating Identity” portion of the limitation. And in Bluetooth, both are independent and optional elements that can exist and perform without the other.

341. As discussed in detail above, in my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification or NOT go with the recommendation provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of

a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

342. The third glaring deficiency in Petitioner’s analysis is that Hiroshi or Kahn or Bluetooth does not support event notification for new data.

343. Petitioner asserts that a thumbnail sent in Hiroshi is an event notification: “a thumbnail and/or data related to the thumbnail would operate as a notification signal.” Petitioner further suggests that “transmission of thumbnails as event notifications.”

344. As discussed above, it is my understanding that the following constructions are agreed by the parties in the District Court:

“data signal notification(s)”	“an indication of the presence of newly acquired data”
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)

345. As discussed in detail above, in Hiroshi (0083) it is clear that the camera receives an instruction/request from the mobile to send a thumbnail. In Hiroshi Step 118, a mobile in a remote control mode sends a instruction request for a thumbnail to the camera, and the camera then responds by sending the requested thumbnail to the phone. It is simple request-response scenario.

346. Also as discussed in detail above, in software design there are two very different categories of application architectures. Request driven and Event Driven.

347. A Request-Driven Architecture uses a synchronous request-response model where a component directly asks for information from another and waits for a response before proceeding. Request-Driven is more suitable for traditional client-server interactions where a direct response is required.

348. An Event-Driven architecture communicates between components by publishing and reacting to events, essentially working asynchronously. Event-Driven architecture is better for real-time, loosely coupled systems that need to react to events as they occur. Key Differences between these two types are discussed in detail above.

349. The Challenged Claims require Enabling “Event Notifications” and sending “Event Notification” to a listener without caring for a response from the

listener, is completely different from the sending a “request and waiting for a response” architecture in BOTH Hiroishi and Kahn.

350. Moreover, as discussed in detail above, the Challenged Claim uses plural for “enabling event notification(S)”. But when the claim is sending the event notification it is for single event “sending event notification”. Reaffirming that it is completely different from single request and single response architecture. Enabling event notifications is done once for multiple events to be received in the future. Unlike simple request response architecture. Petitioner’s argument conflates two vastly different scenarios, which a POSITA would not do.

351. Petitioner relies on the thumbnail transmission instruction as a purported “message to enable event notifications.” (“Hiroishi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images)”; “the mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable event notifications corresponding to the new data”).

352. First, and as discussed above, it is undisputed that Hiroishi clearly says that the referenced “thumbnail transmission instruction” is the information for instructing the transmission of the image data. *See* Hiroishi (Exh. 1011) at [0068] (“Thumbnail transmission instruction information ... is the information for instructing the transmission of the image data showing the thumbnail of the image

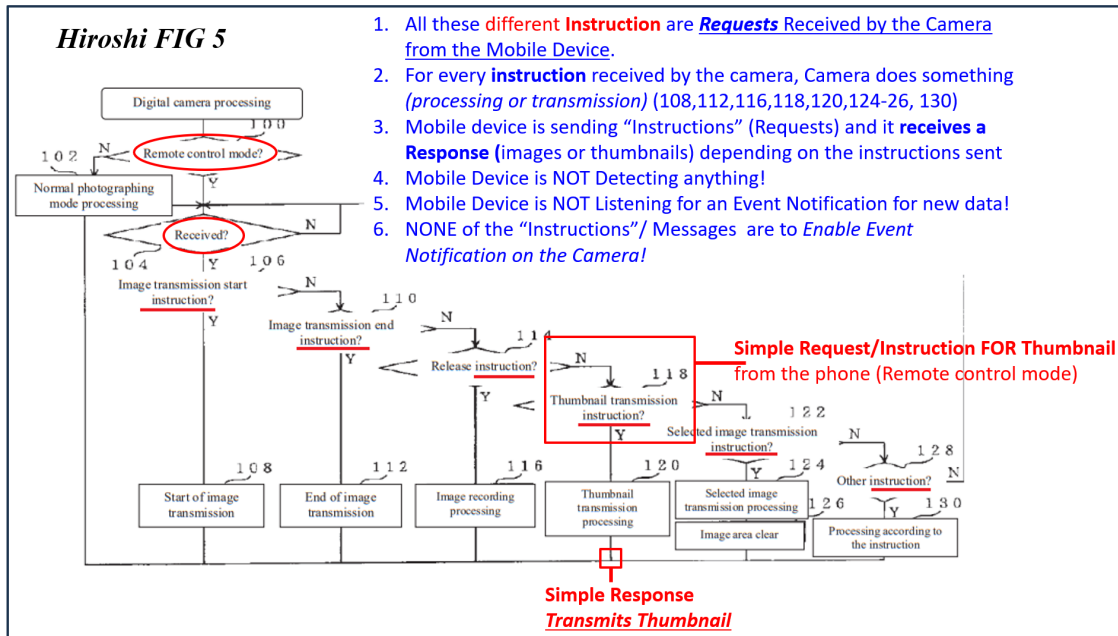
shown according to the digital image data stored in SDRAM 55A”). As such, it is plainly not “to enable event notifications.” (Plural Notifications not single request response).

353. Second, and as discussed above, the “enablement of event notifications” as claimed is a single occurrence, and would not be characterized or satisfied by a transmission associated with each and every new image taken. Under Petitioner’s view; namely, that the transmission of thumbnail instructions is performed “to enable event notifications,” then the process of “enabling event notifications” would be required for every new image requested by the phone. This is plainly not the way in which a POSITA would understand “enabling event notifications” to work, and would wholly defeat the purposes of enabling event notifications in the first place.

354. As discussed above, a reasonable POSITA would have understood that a mobile device sending a “thumbnail transmission instruction” to the camera, followed by the receipt of the thumbnail, is a simple request-response transaction between the two devices that needs to be done for each new thumbnail. It is plainly not an “enabling of event notifications for the new data” by any means. (enabling plural number of notifications is NOT the same as single request response for thumbnail).

355. The word “event” or “event notification” itself does not exist in either Kahn or Hiroshi. This is unsurprising, given the fact that both those state machines are based on request-response architecture. For example, ALL instructions follow the same request-response pattern in Hiroshi and Khan. The phone sends an instruction to the camera and then waits for a response. See Hiroshi at [0092-93]: “In Step 206, image transmission start instruction information is transmitted via the communication unit 49 to the digital camera 50. In response to this, the digital camera 50 performs Step 108 of the digital camera processing (also see FIG. 5) to start an image transmission processing. So, in the following Step 208, [the phone] waits for the reception of the digital image data transmitted from the digital camera 50,”

356. As illustrated in the annotated Figure below (*see* Hiroishi (Exh. 1011) at Fig. 5, as annotated), the process of Hiroishi simply calls for a sequence of instructions sent from the mobile device to the camera:



357. As shown above all the instruction in Hiroshi (108, 112, 116, 118, 120, 124, 126, and 130) follow a simple request-response architecture. For every instruction sent by the mobile device to the camera, the phone waits for the response back from the camera. After receiving the request from the phone, the camera does the processing and transmits the data back for the waiting phone. This is a classic synchronous request-response model, and has NOTHING to do with Event Notifications that are asynchronous in nature.

358. As discussed in detail above, and as a POSITA would have readily understood, a “request-response” model involves a client actively sending a specific request to a server and waiting for a direct response, while an “event notification” is a message sent out when a significant event occurs in a system, allowing any interested components to react asynchronously without needing to

explicitly request the information; essentially, the key difference is that request-response is a direct, synchronous communication while event notification is a broadcast-like, asynchronous communication where the receiver decides when to act upon the information. Support for these assertions can be found in the Exhibit 2010.

359. In request-response, the client initiates communication by sending a request. In event notification, the system generates an event that triggers the notification. Request-response is synchronous, meaning the client waits for the server's response before continuing. Event notification is asynchronous, meaning components can react to events at their own pace. Under that architecture, the mere receipt of a reply to an instruction/request in Hiroshi cannot be reasonably understood as an "event notification" as claimed.

360. As discussed in detail above, Petitioner initially relies on the *thumbnail transmission* as a purported event notification. According to Petitioner, the thumbnail sent in Hiroshi is an event notification.

361. As discussed in detail above, Petitioner's position is untenable, inasmuch as **there is nothing in Hiroishi that performs as an event notification.** Step 118 of receiving a request from the mobile to send a thumbnail and then camera sending the thumbnail to the mobile is NOT an event notification, in any sense of the word for POSITA.

362. As discussed in detail above, Petitioner is not realizing that in any application data model, you have to follow **either** request-response or event-based notification. Here the petitioner and its expert try to combine two orthogonal data architectures. You don't "wait for a response" in an "event notification" architecture. Petitioner himself acknowledges and asserts that Hiroshi is "waiting for a response" just by that logic it cannot be event notification. Because in Event Notification there is NO waiting for a response. Simply put, Hiroshi has very little in common with the teachings and claims of the '381 Patent.

363. Petitioner next contends that "Kahn's teaching of timestamp inclusion with image data underscores the broader concept of event notifications."

364. I am informed and understand that in a related IPR for the '381 Patent, Petitioner asserted "user upload selection" satisfies the "event notification" aspects of the Challenged Claims. *See* '381 Petition (Paper 2) at 39 ("... in the alternative, Kahn teaches the program (applet) configured to listen for an event notification," and "[in reference to] FIG. 5B, a POSITA would have understood that when the user selects upload/upload all, the phone would have listen for a signal from the camera").

365. A POSITA knows that every file that is created on a computer or camera or phone has a timestamp. And a POSITA knows that a timestamp inside a file is not an event notification.

366. Neither Hiroshi nor Kahn has been configured to “listen” to those timestamps. Receiving a file that you requested and that every file has timestamp is not “listening” for a timestamp for a POSITA.

367. On inspection, the word “event” or “event notification” are not found in either Kahn or Hiroshi. As discussed in detail above, both of those state machines are based on request-response architecture. A “request-response” model involves a client actively sending a specific request to a server and waiting for a direct response, while an “event notification” is a message sent out when a significant event occurs in a system, allowing any interested components to react *asynchronously* without needing to explicitly request the information.

368. Kahn (like Hiroshi) is based on a request-response architecture model. There is NO signal to notify, there is NO phone listening for any file timestamp.

369. Next, Petitioner suggests that the “polling” described in Bluetooth is an example of an event notification: “Bluetooth also discusses polling as an example of event notification. For example, polling is described in the active mode, *i.e.*, where both the master and slave actively participate on the channel.”

370. The deficiencies in this argument are many, but primarily it must be recognized that Polling and Event Notification are two very different methods.

They are not examples of one another, they are not related and, in fact, are *conceptual opposites*.

371. As discussed above, I am informed that the parties have agreed on the following constructions in the District Court:

“data signal notification(s)”	“an indication of the presence of newly acquired data”
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)

372. As can be seen from the agreed definition of the terms, data event “notification” and “polling” are very different and the existence of one cannot satisfy the existence of another. A POSITA would readily appreciate the fact that Bluetooth polling in the active mode cannot satisfy the event notification requirements of the claim.

373. Petitioner seems to make another claim in passing, to the effect that “event notification in the Bluetooth specification is sniff mode” without any explanation. This argument has no merit, inasmuch as Bluetooth Sniff mode has nothing to do with notification for new data.

374. The fourth glaring deficiency in Petitioner’s analysis is that Hiroshi and Khan and Bluetooth **do NOT disclose Polling** for new data as required by the **claim 9**.

375. Limitation 9.7 requires: “configured to listen to a polling request from a single mobile client application” , “wherein the polling request is for the new-data.”

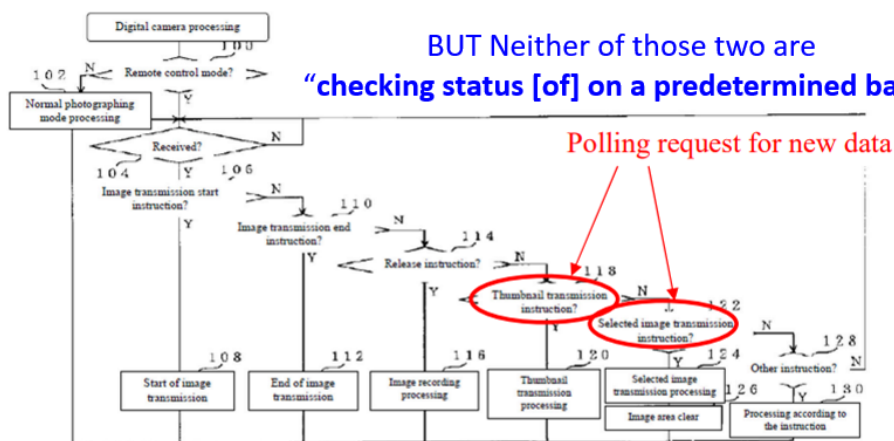
376. Limitation 9.8 requires: “the single mobile client application”, “is configured to” “polling the short-range wireless enabled data capture device.”

377. As noted above, I am informed that the parties have agreed to the following constructions in the District Court:

“poll” / “polling”	“ checking status [of] on a predetermined basis, ” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)
--------------------	--

378. Petitioner argues that “Hiroishi’s thumbnail transmission instruction is a polling request for the new data (images stored in camera memory). TTI-1030, [979]- [985].” I present an annotated version of this figure below:

(FIG. 5)



TTI-1011, FIG. 5 (annotated).

In one example, Hiroishi's thumbnail transmission instruction is a polling request for the new data (images stored in camera memory). TTI-1030, [979]-

379. It is very clear that Hiroishi sending thumbnail instruction to the camera does not satisfy “**checking status [of] on a predetermined basis.**”

Petitioner makes no effort to show that Hiroshi is *checking status* of anything. A request for sending the thumbnail is not checking status, and a request for sending the thumbnail is also not done on a “predetermined basis.”

380. I note that the words “poll” or “Polling” do not exist in Hiroshi.

381. As a final line in its polling section, the Petitioner (without any factual support) asserts that “Hiroishi also discloses this limitation because it uses Bluetooth, which includes polling, to transmit the new data from camera 50 to phone 40. TTI-1030, [979]-[985]; TTI-1011, [0066]- [0067]; TTI-1019, 332.”

382. Petitioner cites to the Bluetooth specification page 332, that is about Link Controller Operation at the data link layer level and has nothing to do with checking the status of any new data. The cited Bluetooth specification TTI-1019 page 332 is talking about “Piconet” to “avoid collisions on the ACL logical transport”. This has nothing to do with checking status of new-data / photos on a predetermined basis.

383. The Petitioner’s reliance on functionality of the ACL Data Link Layer in support of its “polling” argument is unfounded and erroneous. Mobile application has NO DIRECT access to “ACL Logical Data Link Layer” and to “avoid collision” at the Packet Level. As the claim limitation 9.7 and 9.8 require.

384. Moreover, polling to “avoid collision” has nothing to do with “checking status of new data.”

385. The fifth glaring deficiency is that Kahn does NOT teach use of HTTP for uploading photos/media. Instead, it required using WMTP for media upload. As discussed at length and in detail above, HTTP and WMTP are clearly NOT interchangeable.

386. As discussed in detail above, as of 2004, WAP and WMTP were the wireless communication technique, and HTTP were the *standard protocol for the web*. As such, when Kahn says the upload process “occurs via wireless communication technique,” he means wireless WAP and wireless WMTP protocols

(NOT HTTP). Indeed, and as discussed above, Kahn clearly teaches the *exclusive use of WMTP*.

387. Further, and as discussed in detail above, Kahn makes it clear that WMTP is exclusively used for uploading. The result is that Kahn clearly informs the POSITA to use WMTP (which is a wireless protocol, whereas HTTP is and was a web protocol).

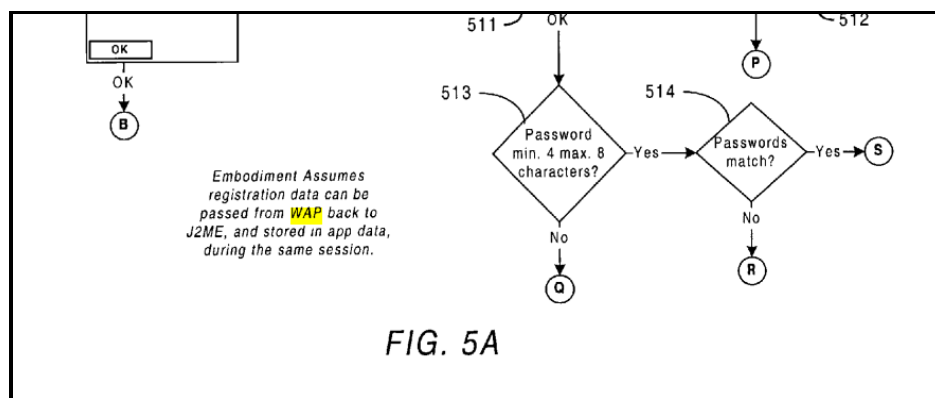
388. As discussed in detail above, Kahn Fig. 5D, element 543, mentions WAP, which was being pushed in the industry at the time (with WMTP). These protocols were specifically designed for mobile devices with limited bandwidth, with WAP acting as a gateway to translate requests from a mobile phone into standard HTTP requests, whereas HTTP (Hypertext Transfer Protocol) is the standard protocol used for web browsing on traditional computers. WMTP and WAP were particularly relevant in the early days of mobile internet when data capabilities were significantly lower. Thus, when Kahn references “wireless communication techniques” in [0057] for “uploading,” it very clearly shows two wireless protocols WMTP and WAP in Fig 5D. It is thus clear that Kahn wants to use wireless protocols like WMTP for upload and NOT web protocol HTTP.

389. As discussed in detail above, Kahn assumes the POSITA knows about WAP architecture and usage in the wireless domain. Just like a POSITA for the wired network would know about TCP/IP or OSI stack, Kahn assumes the POSITA

is knowledgeable about the WAP architecture and WMTTP in the WAP system. Indeed, Kahn talks about wireless transmission techniques and in the detailed diagrams it mentions WMTTP and WAP.

390. As noted and discussed in detail above, a WAP architecture system, the “wireless modular transport protocol” (WMTTP) refers to the Wireless Datagram Protocol (WDP), which acts as the transport layer within the WAP stack, providing a flexible way to transfer data across different network types, even when dealing with unreliable or limited bandwidth connections typical in mobile networks; essentially acting as a modular adaptation layer for various underlying bearer services. As discussed in detail above, it is clear that Kahn intends for the POSITA to use WAP architecture and system. *See Khan at [0017].*

391. Once again, as discussed above, WAP is also described in Kahn **Fig 5A**, it is clear that in Kahn 5A, WAP is used to connect the mobile app (J2ME Applet in 2004) to the outside internet for login registration and password. It is NOT HTTP, but WAP that is used for login password and registration.



392. Still further, and as discussed in detail above, as of 2004, WAP was considered better than HTTP for mobile devices for a variety of reasons, including: (i) optimized for mobile devices; (ii) efficient use of bandwidth; (iii) security; and (iv) adaptation to wireless networks.

393. As further discussed in detail above, to the extent Kahn discussed HTTP, it does so in the context of ecommerce only – not for uploading photos. In addition, Kahn teaches the use of HTTP to obtain GPS data via a location API call. Such is not going out to the server.

394. To reiterate what is discussed in detail above, Kahn is very clear to the POSITA on what protocols to use and where. Specifically: HTTP for e-commerce and internal hardware chip location API. As for uploading/media-transfer and login information, on the other hand, Kahn is very clear to POSITA to use WMTP.

395. As discussed above, Petitioner's assertion that POSITA would use HTTP instead of the clear teaching of WMTP in Kahn for uploading/media-transfer/login is not supported at all in Kahn, and does not reflect the approach to be taken by a POSITA.

396. Moreover, and as discussed in detail above, a POSITA would readily appreciate the fact that WMTP and HTTP are very different protocols and they are NOT Interchangeable. Indeed, WMTP and HTTP run on different layers of the OSI

stack, and there are numerous other significant differences between these two protocols (as discussed above).

2. Ground 2 – Singh 129 in View of Singh 906

397. David Lett suggests that a POSITA would have been motivated to combine the teachings of Singh 129 in view of Singh 906 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

398. First, I have examined the scope and content of the cited prior art. With respect to teachings of Singh 129 and Singh 906, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Singh 129 in view of Singh 906 purportedly render the Challenged Claims obvious. I disagree David Lett's conclusions. Here, I address the most glaring deficiencies in his analysis.

399. Petitioner asserts that the Examiner's withdrawal of the written description rejection during prosecution was error because the Examiner "did not analyze whether the applicants were in possession of the claimed combinations of elements that mix and match features from unrelated patent applications."

400. As I understand, the main complaint from the Petitioner for Ground 2 has been about the "client application using HTTP to upload such user information or global positioning information to a user data publishing website" limitation.

401. I have reviewed Singh 129, Singh 906, and the related prosecution histories, and note the following:

402. In my opinion, the Examiners' own Notice of Allowance shows that the Examiner not only understood the scenario but actually proposed his own amendments for HTTP and GPS.

403. As I understand, it was the Examiner who initiated the Interview on September 3, 2021, and the Examiner wanted to incorporate the aspects of Claim 7 into independent claim 1. As I further understand, the Examiner himself proposed the narrowing of the claim's limitation and proposed to incorporate the "HTTP sending Global Positioning System information" of Claim 7 into Claim 1.

404. That material is clearly from the incorporated reference specification and the Examiner must have understood that, as there is **no** mention of GPS information in the original specification, but *only* in the incorporated reference.

Attachment(s)	
1. ☒ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material	7. ☐ Other _____
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date, 9/3/21.	
/SULAIMAN NOORISTANY/ Primary Examiner, Art Unit 2415	
U.S. Patent and Trademark Office PTOL-37 (Rev. 08-13)	
<u>Notice of Allowability</u>	
Part of Paper No./Mail Date 20210907	

<u>Examiner-Initiated Interview Summary</u>	Application No. 16/532,507	Applicant(s) Singh et al.		
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (First Inventor to File) Status No	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
SULAIMAN NOORISTANY	Primary Examiner	Telephonic
Ashok Tankha	Attorney	

Date of Interview: 03 September 2021

Issues Discussed:

Proposed Amendment(s)

As an initial matter, Examiner initiated an interview with Mr. Ashok Tankha to expedite prosecution of the present application. During the interview, an overview of the invention was presented and proposed claim amendments were discussed (e.g., incorporating claim 7 into claim 1), which Examiner indicated appear to overcome the outstanding grounds of rejection and put the application in forward status. Thus, formal agreement was reached during the interview.

cellular data network, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is ~~at least one of~~ no wait automatic[,] or wait X minutes automatic, ~~and wait for user input~~, wherein the single mobile client application for the short-range wireless enabled cellular phone is further configured to use the HTTP to send a user preference to the user data publishing website over the cellular data network, wherein the user preference comprises global positioning system information, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Summary of telephone conversation on September 3, 2021

Applicant thanks the examiner for proposing examiner's amendments during the telephonic conversation on September 3, 2021 to put the application in a condition for allowance.

Follow up by the applicant

As suggested by the examiner, applicant has included the limitation of claim 7 in claims 1 and 4 and cancelled claim 7. Furthermore, as suggested by the examiner, applicant has included the limitation of claim 14 in claims 8 and 12 and cancelled claim 14.

Claim 7 (previously presented): The system of claim 4, wherein the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to:

6

use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information.

405. Shown above is the Claim 7 that the Examiner wanted to include in the original claim after he himself initiated the interview. One would have to safely assume that he did his analysis and then initiated the interview and wanted the applicant to narrow the claims. He is the one who proposed HTTP with GPS from Singh 906 into the patent claims. To say that the examiner did not analyze whether the applicants were in possession of the claimed combinations from the

incorporated reference, when the examiner in its own Notice of Allowance and his own initiated interview proposed an amendment that is from the incorporated reference seems highly unlikely and contrary to the presumptions that Examiners perform their jobs properly.

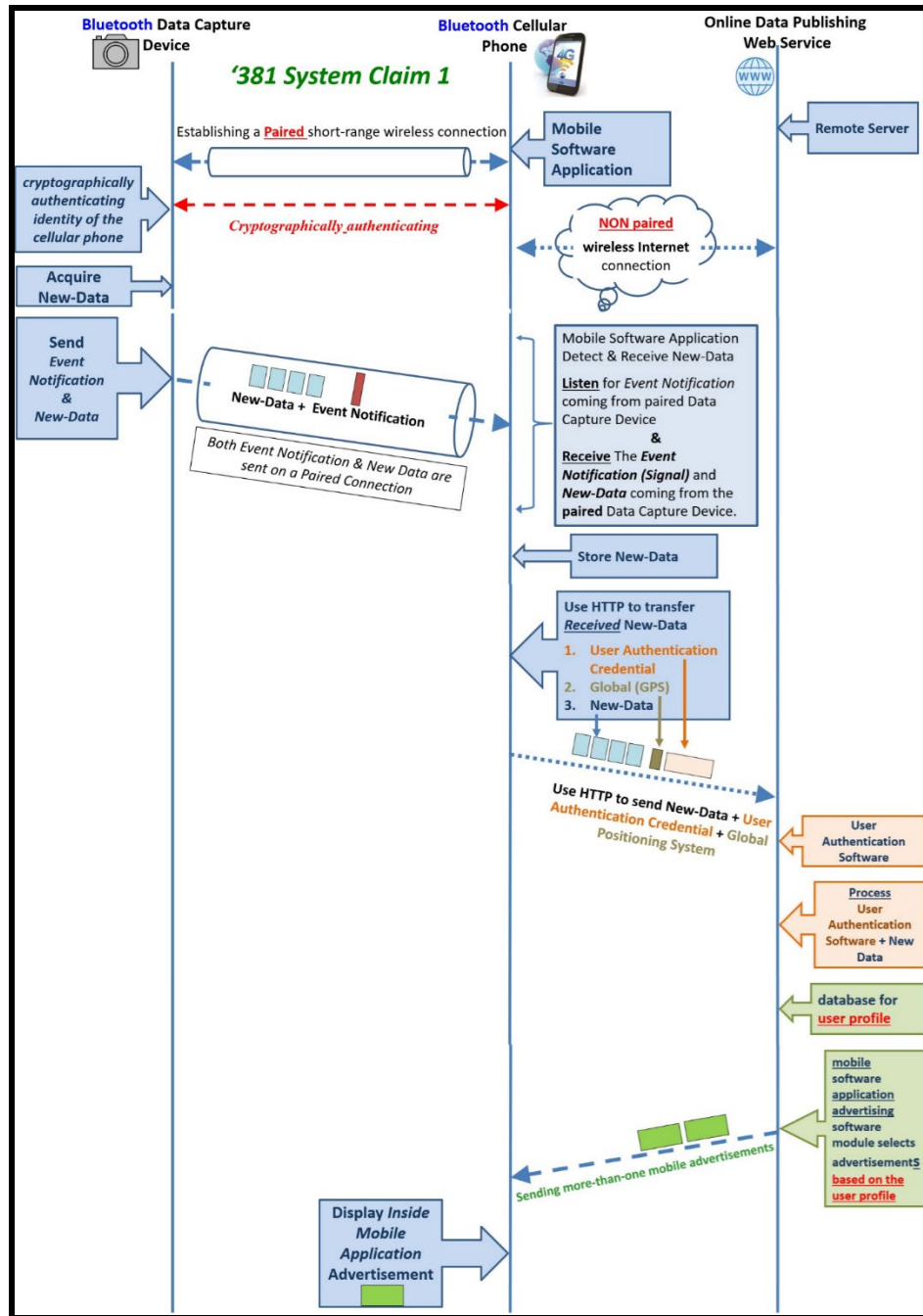
D. Validity Analysis of the ‘381 Patent

1. Ground 1 – Hiroishi, Kahn, and Bluetooth

406. David Lett suggests that a POSITA would have been motivated to combine the teachings of Hiroishi in view of Kahn, Endsley, and Bluetooth in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

407. First, I have examined the scope and content of the cited prior art. With respect to teachings of Hiroishi, Kahn, Endsley, and Bluetooth, David Lett provides a claim-by-claim articulation of his thoughts regarding how the Hiroishi in view of Kahn, Endsley, and Bluetooth purportedly render the Challenged Claims obvious. I disagree David Lett’s conclusions. Here, I address the most glaring deficiencies in his analysis.

408. As an initial point of reference, I provide the following detailed flow diagram (prepared by Cellspin in an earlier filing), which I believe accurately illustrates the connectivity and data flow as variably recited in the Challenged Claims (using Claim 1 of the ‘381 Patent as an example):



409. The first glaring deficiency in Petitioner's analysis is that (as discussed above), I understand the parties in the District Court have agreed to the constructions of the following key terms:

“after the paired secure Bluetooth connection is established” /	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device” /
“after establishing a paired Bluetooth connection”	“after the paired connection is established and maintained on a continuous basis between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone”
“after establishing the short-range paired wireless connection” / “after the short-range paired wireless connection is established”	“after the paired connection is established and maintained on a continuous basis between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone”

410. Neither Hiroshi, Kahn or Bluetooth disclose a paired connection that is “established and maintained on a continuous basis.” As discussed above, I understand the Board rejected that construction in its institution decision because of material presented to them on the record.

411. The Petitioner has not asserted anywhere in any of these 4 cases that the prior art discloses a “**paired connection is established and maintained on a continuous basis.**”

412. Indeed, NONE of the cited prior art (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone paired connection is “established and maintained on a continuous basis.”

413. As discussed in detail above, as of 2007 a POSITA would definitely NOT “maintain a paired connection on a continuous basis.” The agreed claim construction (with which I also agree) is “after the paired connection is established and maintained on a continuous basis.”

414. The second glaring deficiency in Petitioner’s analysis is that “pairing” is not a “must” for a Bluetooth connection as suggested by the Petitioner and its expert, and both Pairing and Cryptographic Authentication are Non-Obvious.

415. The Petition asserts that in Hiroishi: “For the mobile phone and the camera to communicate via Bluetooth, the mobile phone and the **camera must have been “paired,”** *but this is without any factual support for the “must”* requirement. Given that Bluetooth never says pairing is a default or pairing is required/must. Contrary to Davit Lett and Petitioner’s assertion the Bluetooth Specification is very clear that Pairing is not required for Bluetooth devices to communicate and Pairing is optional.

416. As noted and discussed in detail above, in Bluetooth “Pairing” is different from “Authentication” and both are different from “Encryption. As shown and discussed above, there are 15 different **optional** activities after a Bluetooth connection is established. Pairing, Authentication, and Encryption are different optional activities. Also, as shown in Figure 3.1 in the v2.1+EDR Bluetooth Core

Specification [Exhibit TTI 1019, p. 861] it again clearly shows that the Pairing is different from Authentication and both of them are different from Encryption.

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 0]		page 19 of 74
		 Bluetooth
2.1	Remote Name Request.....	685
2.2	One-time Inquiry.....	687
2.3	Periodic Inquiry	689
3	ACL Connection Establishment and Detachment.....	691
3.1	Connection Setup	692
4	Optional Activities After ACL Connection Establishment.....	699
4.1	Authentication Requested.....	699
4.2	Simple <u>Pairing</u> Message Sequence Charts.....	700
4.3	Link Supervision Timeout Changed Event.....	713
4.4	Set Connection Encryption.....	714
4.5	Change Connection Link Key.....	715
4.6	Change Connection Link Key with Encryption Pause and Resume.....	715
4.7	<u>Master Link Key</u>	717
4.8	Read Remote Supported Features	719
4.9	Read Remote Extended Features.....	719
4.10	Read Clock Offset.....	720
4.11	Role Switch on an <u>Encrypted Link using Encryption</u> Pause and Resume.....	720
4.12	<u>Refreshing Encryption Keys</u>	721
4.13	Read Remote Version Information	722
4.14	QOS Setup.....	722
4.15	Switch Role	723

All 15 are
Optional

3 ACL CONNECTION ESTABLISHMENT AND DETACHMENT

A flow diagram of the establishment and detachment of a connection between two devices is shown in Figure 3.1 on page 691. The process is illustrated in 9 distinct steps. A number of these steps may be optionally performed, such as authentication and encryption. Some steps are required, such as the Connection Request and Setup Complete steps. The steps in the overview diagram directly relate to the steps in the following message sequence charts.

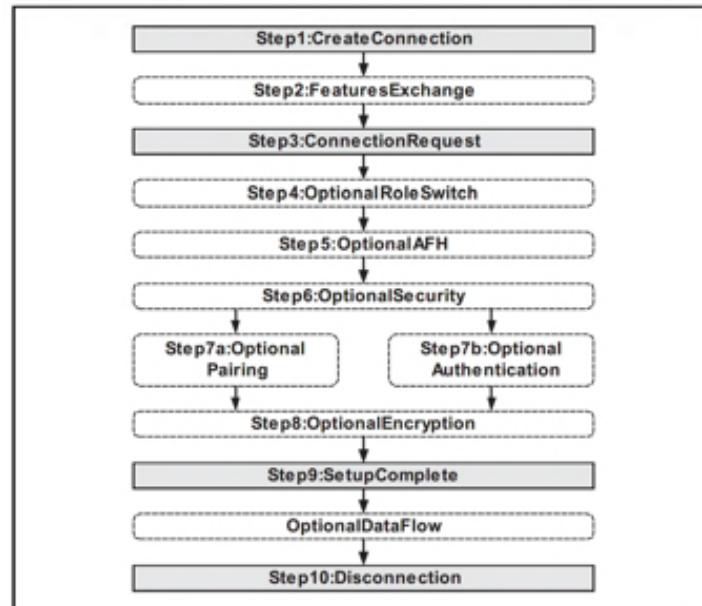


Figure 3.1: Overview diagram for connection setup.

417. For POSITA these options are chosen for a connection depending on the requirements of the solution being implemented. In the Bluetooth family of specifications, Profile specifications are used to describe how to implement a particular use case or family of related use cases. POSITA would listen to recommendations from the v2.1+EDR Bluetooth Core specification or the Bluetooth Basic Imaging Profile (BIP) specification.

418. Moreover, Hiroshi [0067] teaches one to follow the Bluetooth Standards: “Therefore, the communication unit 49 of the mobile phone 40 and the communication unit 59 of the digital camera 50 are configured so as to allow a

communication according to the standard of Bluetooth, respectively.” For Petitioner to suggest otherwise is contrary to Hiroishi’s teaching.

419. Again, and as noted and discussed above, the Bluetooth specification clearly states twice that, “[w]hen both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption.” (Exhibit TTI 1019, p. 1273 and 1286).

420. This statement also means that NOT ALL Bluetooth devices supported pairing. (Conditional statement when both device).

421. As discussed above, as of 2007 a POSITA understood that the Basic Imaging Profile (BIP) describes all the Kahn, Hiroishi, Feinberg, Endsley scenarios. However, BIP did not require a paired Bluetooth connection for all these scenarios. For the scenarios most in line with Kahn, Hiroishi, Feinberg, Endsley scenarios, *i.e.* pull based or push based image transfer, BIP was not recommending using a paired Bluetooth connection.

422. NONE of the cited references (Kahn, Hiroishi, Feinberg, Endsley) even mention the word “pair” or “pairing,” let alone the timing for pairing as recited in the Challenged Claims. Applications and systems would connect to Bluetooth and then disconnect after the job was done. The v2.1+EDR Bluetooth Core Specification lists many optional activities, with Pairing and Authentication being only some of them, and neither were the default *for any scenarios*. Data

Encryption between the two devices was the default option in 2007, not Pairing and not Authenticated.

423. As discussed in detail above, in my opinion, Petitioner and David Lett are relying upon hindsight reasoning to suggest that a POSITA would NOT go with the Default option provided by the Bluetooth Standard of 2007. According to Petitioner and David Lett, a POSITA would NOT listen to the v2.1+EDR Bluetooth Core specification or NOT go with the recommendation provided by the Bluetooth Basic Imaging Profile (BIP) specification, and furthermore would NOT care about pairing disadvantages, such as a poor user experience and battery drain. In my opinion, such hindsight is not warranted and does not reflect the thought process of a POSITA. Even today, a POSITA puts a lot of weight and follows the Bluetooth standards body recommendations. There is reason for the standard bodies to come up with default recommendation, because that is what the latest and best understanding of the problem and the solutions are at the time. To suggest that a POSITA would proceed in a manner that was not being recommended by any standard body is not supported and is unreasonable.

424. The third glaring deficiency in Petitioner's analysis is that none of Hiroshi or Kahn or Bluetooth support event notification for new data.

425. Petitioner asserts that the thumbnail sent in Hiroishi is an event notification: "POSITA would have also understood that the thumbnails of Hiroishi

being sent to the phone from the camera constitute the signal representing the event notification.”

426. As noted and discussed above, it is my understanding that the parties have agreed upon certain constructions in the District Court, including:

“data signal notification(s)”	“an indication of the presence of newly acquired data”
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)

427. In Hiroshi (at [0083]) it is clear that the camera receives an instruction/request from the mobile to send a thumbnail: “If no in Step 118, *i.e.*, when the instruction information received from the mobile phone 40 in Step 104 is not the thumbnail transmission instruction information, the process goes to Step 122.”

428. In Hiroishi Step 118, a mobile in a remote control mode sends a instruction request for a thumbnail to the camera, and the camera then responds by sending the requested thumbnail to the phone. It is simple request-response scenario.

429. As discussed in detail above, in software design there are two very *different* categories of application architectures. **Request driven and Event Driven.**

430. As noted and discussed in detail above, there are a number of important distinctions, with Request-Driven Architecture using a **synchronous** request-response model where a component directly asks for information from another *and waits for a response* before proceeding. Request-Driven is more suitable for traditional client-server interactions where a direct response is required.

431. An Event-Driven architecture communicates between components by publishing and reacting to events, essentially working **asynchronously**. Event-Driven architecture is better for real-time, loosely coupled systems that need to react to events as they occur.

432. Key Differences are: Communication Pattern for Event-Driven: Publishes/sends events that any interested component can subscribe/listen to and process/react to asynchronously. Communication Pattern for Request-Driven: Sends direct requests to a specific component and waits for a response.

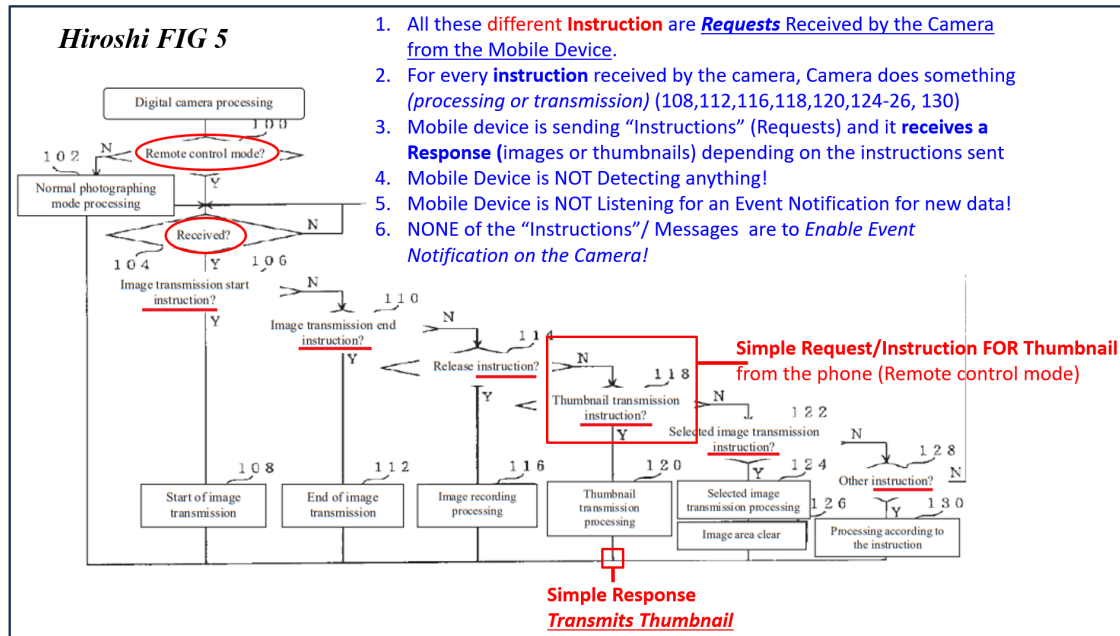
433. As discussed in detail above, support for these assertions can be found in the Exhibit 2010.

434. The Challenged Claims require sending “Event Notification” to a listener without caring for a response from the listener, is completely different from sending a “request and waiting for a response” architecture in BOTH Hiroshi and Kahn.

435. The word “event” or “event notification” itself does not exist in either Kahn or Hiroshi! Both those state machines are based on request-response architecture.

436. For example, ALL instructions follow the same request-response pattern in Hiroshi and Khan. Phone sends an instruction to the camera and then waits for a response. Hiroshi “(0092) In Step 206, image transmission start **instruction** information **is transmitted** via the communication unit 49 **to the digital camera** 50. In response to this, the digital camera 50 performs Step 108 of the digital camera processing (also see FIG. 5) to start an image transmission processing. (0093) So, in the following Step 208, **[the phone] waits for** the reception of the digital image **data transmitted from the digital camera** 50,”

437. As illustrated in the annotated Figure below (*see* Hiroishi (Exh. 1011) at Fig. 5, as annotated), the process of Hiroishi simply calls for a sequence of instructions sent from the mobile device to the camera.



438. As shown above, all the instruction in Hiroshi (108, 112, 116, 118, 120, 124, 126, and 130) follow a simple request-response architecture. For every instruction sent by the mobile device to the camera, the phone waits for the response back from the camera. After receiving the request from the phone, the camera does the processing and transmits the data back for the waiting phone. This is a classic synchronous request-response model, and has NOTHING to do with Event Notifications that are asynchronous in nature.

439. As discussed in detail above, and as a POSITA would have readily understood, a "request-response" model involves a client actively sending a specific request to a server and waiting for a direct response, while an "event notification" is a message sent out when a significant event occurs in a system, allowing any interested components to react asynchronously without needing to

explicitly request the information; essentially, the key difference is that request-response is a direct, synchronous communication while event notification is a broadcast-like, asynchronous communication where the receiver decides when to act upon the information. Support for these assertions can be found in the Exhibit 2010.

440. In request-response, the client initiates communication by sending a request. In event notification, the system generates an event that triggers the notification. Request-response is synchronous, meaning the client waits for the server's response before continuing. Event notification is asynchronous, meaning components can react to events at their own pace. Under that architecture, the mere receipt of a reply to an instruction/request in Hiroshi cannot be reasonably understood as an "event notification" as claimed.

441. As discussed in detail above, Petitioner initially relies on the *thumbnail transmission* as a purported event notification. According to Petitioner, the thumbnail sent in Hiroshi is an event notification.

442. As discussed in detail above, Petitioner's position is untenable, inasmuch as **there is nothing in Hiroishi that performs as an event notification.** Step 118 of receiving a request from the mobile to send a thumbnail and then camera sending the thumbnail to the mobile is NOT an event notification, in any sense of the word for POSITA.

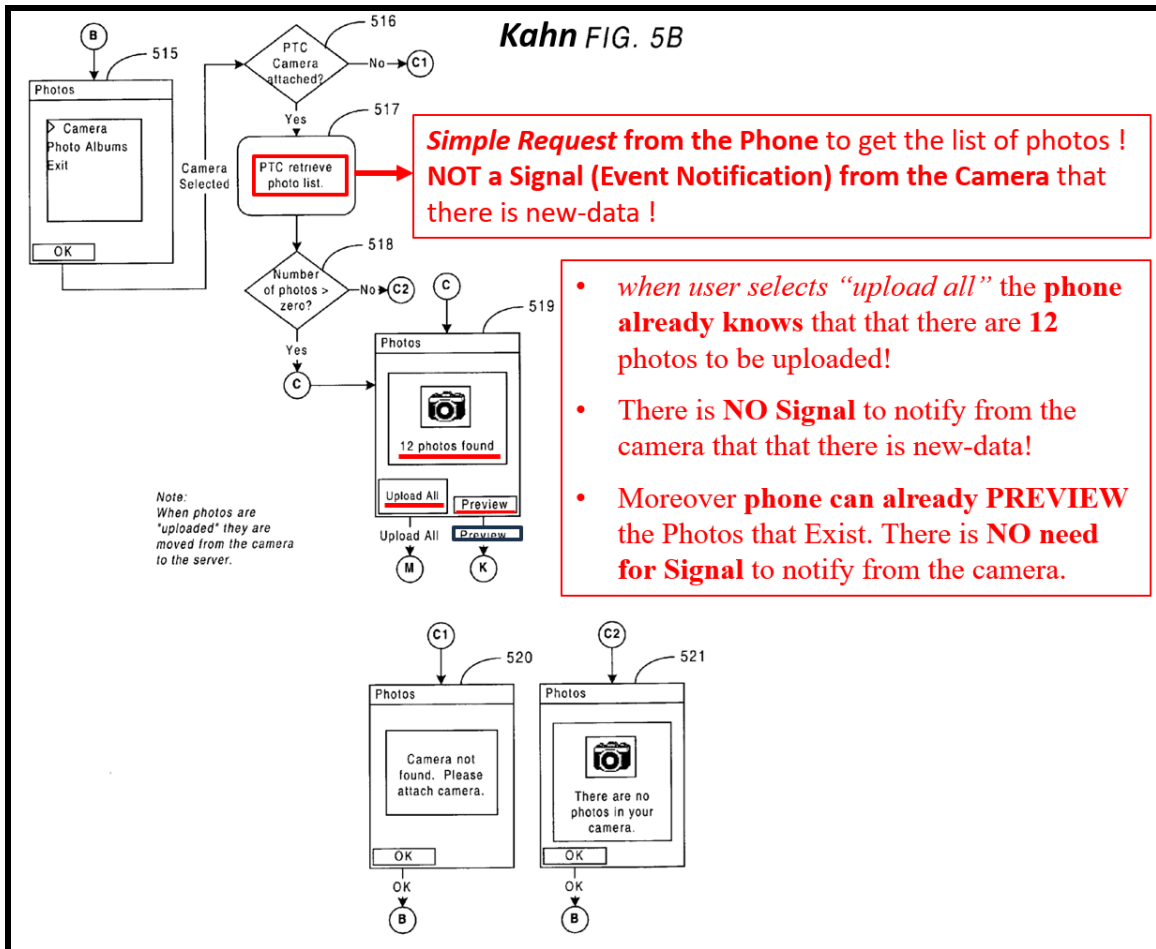
443. As discussed in detail above, Petitioner is not realizing that in any application data model, you have to follow **either** request-response or event-based notification. Here the petitioner and its expert try to combine two orthogonal data architectures. You don't "wait for a response" in an "event notification" architecture. Petitioner himself acknowledges and asserts that Hiroshi is "waiting for a response" just by that logic it cannot be event notification. Because in Event Notification there is NO waiting for a response. Simply put, Hiroshi has very little in common with the teachings and claims of the '381 Patent.

444. Petitioner next contends that "Kahn's teaching of timestamp inclusion with image data underscores the broader concept of event notifications."

445. Petitioner next contends that the disclosure in Kahn of a user upload selection satisfies the "event notification" aspects of the Challenged Claims: ("... in the alternative, Kahn teaches the program (applet) configured to listen for an event notification," and "[in reference to] FIG. 5B, a POSITA would have understood that when the user selects upload/upload all, the phone would have listen for a signal from the camera") and ("timestamp described in Kahn is used in the combination as an event notification because it is a signal that") and ("the event notification (timestamp) and acquired new-data (full resolution images) are received by the mobile phone").

446. The word “event” or “event notification” itself does not exist in either Kahn or Hiroshi, and both those state machines are based on request-response architecture. As noted above, a “request-response” model involves a client actively sending a specific request to a server and waiting for a direct response, while an “event notification” is a message sent out when a significant event occurs in a system, allowing any interested components to react *asynchronously* without needing to explicitly request the information. Support for these assertions can be found in the Exhibit 2010.

447. Kahn (like Hiroshi) is based on a request-response architecture model. In Khan Fig 5 B (517 step) there is a simple request from the phone to get the list of photos from the camera and then the phone get a response from the camera that has the list of photos (12 photos found, as shown in the Fig 5B). It is a simple request-response model. There are no event notifications or signal to notify of any kind. There is NO listening for any events. The state machine is clear; every time the **phone** sends a “PTC retrieve the photo list” **request** to the camera, the **camera sends a response** to the mobile device with the list.



448. When the user selects the mobile GUI element “upload all” the phone uploads all 12 photos. There is NO signal to notify, there is NO phone listening for any file timestamp. The word “listen” does not even exist in Kahn.

449. Next, Petitioner also argues that the “polling” described in Bluetooth is an example of an event notification: “In Bluetooth *polling*, the slave device (the camera) has to send an AR_ADDR message to the master device;” and identifying the “AR_ADDR message that the slave sends when it wants to send data,” and “During polling, the slave device must respond to a polling request”). The

deficiencies in this argument are many, but (as discussed in detail above) primarily it must be recognized that Polling and Event Notification are two very different methods. They are not examples of one another, they are not related and, in fact, are *conceptual opposites*.

450. Again, and as noted above, it is my understanding that the parties in the District Court have agreed to the following:

“data signal notification(s)”	“ an indication of the presence of newly acquired data ”
“poll” / “polling”	“ checking status [of] on a predetermined basis, ” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)

451. As can be seen from the agreed definition of the terms, data event “notification” and “polling” are very different and the existence of one cannot satisfy the existence of another. The Bluetooth polling and AR_ADDR cannot satisfy the event notification requirements of the claim.

452. The fourth glaring deficiency in Petitioner’s analysis is that Hiroshi and Bluetooth **do NOT disclose Polling** for new data as required by the claims.

453. It is my understanding that the following have been agreed by the parties in the District Court:

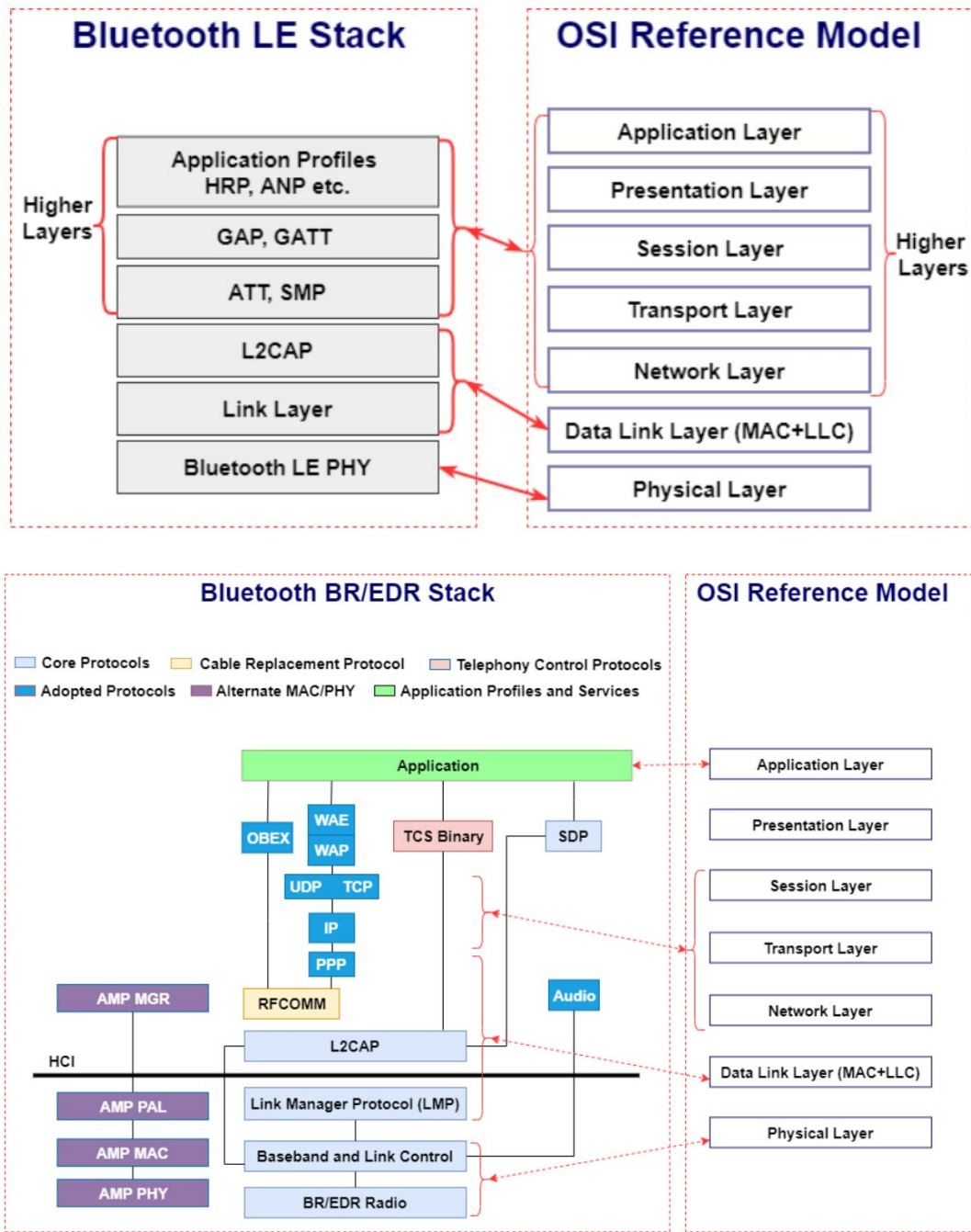
“poll” / “polling”	“checking status [of] on a predetermined basis,” where “predetermined” refers to programming that sets the frequency of the status checks (e.g., at set intervals, dynamic intervals, randomly, etc.)
--------------------	--

454. Petitioner argues that “Hiroishi teaches sending, from the program running on the mobile phone, a thumbnail instruction to the camera, which is a polling instruction.” (citing Ex. 1011 (Hiroishi) ¶¶ 81, 84, 102, Figs. 5–6).

455. But it is very clear that Hiroshi sending thumbnail instruction to the camera does not satisfy the required claim construction **“checking status [of] on a predetermined basis.”** Petitioner makes no effort to show that Hiroshi is *checking status* of anything. A request for sending the thumbnail is not checking status of anything. A request for sending the thumbnail is also not done on a “predetermined basis.”

456. Challenged Claim 12 recites: “said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data.” The claim language is very clear that the same mobile application that is doing HTTP is also doing the polling: “wherein polling comprises sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer.” For a POSITA, it is very clear that a mobile application that does HTTP based transfer and polling for new data at the application layer, it does not have direct access to any data link layer attributes.

457. Shown below are the Bluetooth protocol mapping to OSI stack Math works. *See www.mathworks.com/help/bluetooth/ug/bluetooth-protocol-stack.html:*



458. In the preceding figure, the Bluetooth protocol stack is shown along with the OSI reference model. There is one-to-one mapping at the physical layer

(PHY). The OSI data link layer (DLL) maps to the Bluetooth LE logical link control and adaptation protocol (L2CAP) and link layer (LL). In the Bluetooth stack, the higher layers provide application layer services, device roles and modes, connection management, and security protocol. The functionality of the Bluetooth protocol stack is divided between three main layers: the Controller, the Host, and Application Profiles and Services.

459. Again it is very clear to a POSITA from the OSI mapping of Bluetooth, that a mobile application that does HTTP based transfer at the application layer, it does **NOT have any direct access to any data link layer attributes of Bluetooth.**

460. Petitioner relies on functionality of the ACL Data Link Layer in support of its “polling” argument: “Bluetooth teaches that ‘*to avoid collisions* on the ACL *logical transport*, a slave is only allowed to transmit when addressed by the LT_ADDR in the packet header in the preceding master-to-slave slot’” and “Bluetooth uses *polling* to, *e.g.*, control slave transmissions to *avoid collisions* on the *transport channel*.” This position is unsupported and incorrect. The mobile application has NO DIRECT access to “ACL Logical Data Link Layer” and to “avoid collision” at the Packet Level.

461. Moreover, polling to “avoid collision” has nothing to do with “checking status of new data.”

462. The fifth glaring deficiency in Petitioner's analysis is that Kahn does NOT teach use of HTTP for uploading photos/media. Instead, it required using WMTTP for media upload. As discussed at length and in detail above, HTTP and WMTTP are clearly NOT interchangeable.

463. As discussed in detail above, as of 2004, WAP and WMTTP were the wireless communication technique, and HTTP were the *standard protocol for the web*. As such, when Kahn says the upload process "occurs via wireless communication technique," he means wireless WAP and wireless WMTTP protocols (NOT HTTP). Indeed, and as discussed above, Kahn clearly teaches the *exclusive use of WMTTP*.

464. Further, and as discussed in detail above, Kahn makes it clear that WMTTP is exclusively used for uploading. The result is that Kahn clearly informs the POSITA to use WMTTP (which is a wireless protocol, whereas HTTP is and was a web protocol).

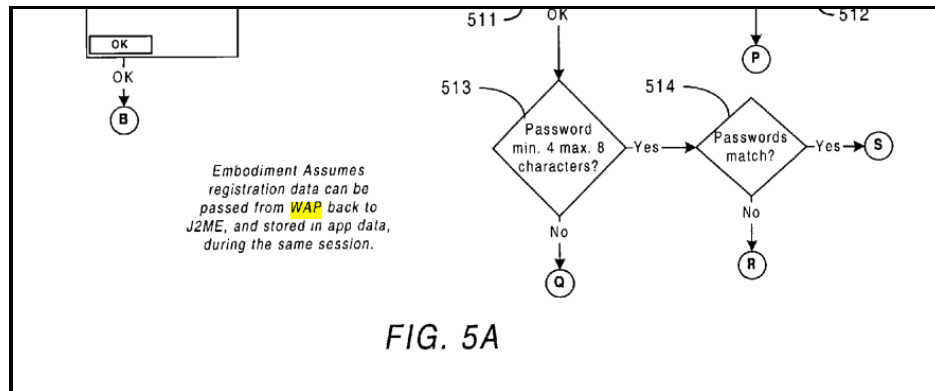
465. As discussed in detail above, Kahn Fig. 5D, element 543, mentions WAP, which was being pushed in the industry at the time (with WMTTP). These protocols were specifically designed for mobile devices with limited bandwidth, with WAP acting as a gateway to translate requests from a mobile phone into standard HTTP requests, whereas HTTP (Hypertext Transfer Protocol) is the standard protocol used for web browsing on traditional computers. WMTTP and

WAP were particularly relevant in the early days of mobile internet when data capabilities were significantly lower. Thus, when Kahn references “wireless communication techniques” in [0057] for “uploading,” it very clearly shows two wireless protocols WMTP and WAP in Fig 5D. It is thus clear that Kahn wants to use wireless protocols like WMTP for upload and NOT web protocol HTTP.

466. As discussed in detail above, Kahn assumes the POSITA knows about WAP architecture and usage in the wireless domain. Just like a POSITA for the wired network would know about TCP/IP or OSI stack, Kahn assumes the POSITA is knowledgeable about the WAP architecture and WMTP in the WAP system. Indeed, Kahn talks about wireless transmission techniques and in the detailed diagrams it mentions WMTP and WAP.

467. As noted and discussed in detail above, a WAP architecture system, the “wireless modular transport protocol” (WMTP) refers to the Wireless Datagram Protocol (WDP), which acts as the transport layer within the WAP stack, providing a flexible way to transfer data across different network types, even when dealing with unreliable or limited bandwidth connections typical in mobile networks; essentially acting as a modular adaptation layer for various underlying bearer services. As discussed in detail above, it is clear that Kahn intends for the POSITA to use WAP architecture and system. *See Khan at [0017].*

468. Once again, as discussed above, WAP is also described in Kahn **Fig 5A**, it is clear that in Kahn 5A, WAP is used to connect the mobile app (J2ME Applet in 2004) to the outside internet for login registration and password. It is NOT HTTP, but WAP that is used for login password and registration.



469. Still further, and as discussed in detail above, as of 2004, WAP was considered better than HTTP for mobile devices for a variety of reasons, including: (i) optimized for mobile devices; (ii) efficient use of bandwidth; (iii) security; and (iv) adaptation to wireless networks.

470. As further discussed in detail above, to the extent Kahn discussed HTTP, it does so in the context of ecommerce only – not for uploading photos. In addition, Kahn teaches the use of HTTP to obtain GPS data via a location API call. Such is not going out to the server.

471. To reiterate what is discussed in detail above, Kahn is very clear to the POSITA on what protocols to use and where. Specifically: HTTP for e-commerce

and internal hardware chip location API. As for uploading/media-transfer and login information, on the other hand, Kahn is very clear to POSITA to use WMTP.

472. As discussed above, Petitioner's assertion that POSITA would use HTTP instead of the clear teaching of WMTP in Kahn for uploading/media-transfer/login is not supported at all in Kahn, and does not reflect the approach to be taken by a POSITA.

473. Moreover, and as discussed in detail above, a POSITA would readily appreciate the fact that WMTP and HTTP are very different protocols and they are NOT Interchangeable. Indeed, WMTP and HTTP run on different layers of the OSI stack, and there are numerous other significant differences between these two protocols (as discussed above).

474. The sixth glaring deficiency in Petitioner's analysis is that Kahn does NOT teach a database, wherein *the database stores a user profile*. As discussed in detail above, a POSITA would understand "user profile" as "*a collection of information associated with a user. It contains information such as their Username, Password, Email, Age, Gender, Country/Address,*" and Petitioner has not shown that those set of six attributes are stored in any metadata database in Kahn.

475. The Petition relies on Kahn at [0098] for support for “user profile” database. There is no mention of “*user profile*” anywhere in Kahn, nor is there any disclosure of *Username, Password, Email, Age, Gender, Country/Address* in Kahn.

476. To the extent Kahn mentions “metadata,” this does not satisfy the limitation because metadata has no mention of the ALL the required attributes for the most basic user profile. Petitioner relies ONLY on “location” as an attribute for user profile, which is insufficient. The only mention of “location” as metadata in Kahn simply does not inform a POSITA of the existence of any “user profile.”

477. Petitioner asserts that “On the other hand, the metadata, including the location ID, is stored as a database record in a database table in the metadata database. The database table is keyed by a unique element (image) ID, and also includes fields for user ID, timestamp (date/time), and location ID (longitude and latitude decimal values). That the database is keyed for user ID means that the database stores user profile.” I disagree with Petitioner.

478. Petitioner quotes the Kahn text that database is keyed to image ID. Then in the very next line, petitioner erroneously suggests that the database is keyed to user ID. **But Kahn plainly says it is keyed to image ID and NOT keyed to user ID**. The user ID, timestamp (date/time), and location ID are just attributed for the Image(photo). The difference is illustrated below of what Kahn teaches and what is actually required under the properly construed claim:

Kahn Database prior-art			
Unique Element (Key)	Location ID	Time Stamp	User ID
Unix File name (pointer/hash)	Long/Lat	(date/time)	
Image_ID_1	123/789	Date-1-Time-1	User-ID-XX
Image_ID_2	123/456	Date-2-Time-2	User-ID-XX
Image_ID_3	123/789	Date-1-Time-1	User-ID-YY
Image_ID_4	234/781	Date-2-Time-2	User-ID-YY
Image_ID_5	123/456	Date-2-Time-2	User-ID-YY

User-Profile Database should at least look like						
User ID (Key)	Username	Password	Address	Gender	Age	Email Address
User_ID_1	John	Abc111xy	US	M	42	John42@xxx.com
User_ID_2	Mary	Xyz234ab	Canada	F	34	mary@yyy.com
User_ID_3	Bob	Yy4569df	US	M	37	bob@zzz.com
User_ID_4	Sofia	Cfty9900	Canada	F	37	Sofia23@rrr.com
User_ID_5	Emma	Ntc456yt	US	F	42	Emmaa22@aaa.com

479. The words “user profile” do NOT exist in Kahn. Just the mention of user ID in the image database would not satisfy the claim requirement when properly construed (as discussed in detail above). Again, the user profile comprising *Username, Password, Email, Age, Gender, Country* has **not** been shown anywhere in Kahn, and no database in Kahn exists with those six attributes.

480. Even if a separate location metadata database exists in Kahn, Petitioner has not shown that Kahn image metadata has all the basic attributes needed for the user profile (as properly construed).

481. The seventh glaring deficiency in Petitioner’s analysis is that Kahn advertisements are NOT based on the user profile. Given a proper construction of “user profile” (as discussed in detail above) as “*a collection of information associated with a user. It contains information such as their Username, Password,*

Email, Age, Gender, Country/Address,” then Petitioner has **not** shown that advertisement as disclosed in Kahn are based on the user profile.

482. Because Kahn does not have a “user profile” as required, then the ads sent to the WAP, Email or the like in Kahn cannot be based on the non-existent user profile.

2. Ground 2 – Singh 129 in View of Singh 906

483. David Lett suggests that a POSITA would have been motivated to combine the teachings of Singh 129 in view of Singh 906 in order to arrive at the inventions of the Challenged Claims. For a variety of reasons, I disagree.

484. First, I have examined the scope and content of the cited prior art. With respect to teachings of Singh 129 and Singh 906, David Lett provides a claim-by-claim articulation of his thoughts regarding how Singh 129 in view of Singh 906 purportedly renders the Challenged Claims obvious. I disagree David Lett’s conclusions. Here, I address the most glaring deficiencies in his analysis.

485. Petitioner makes an unfounded assertion that the Examiner’s withdrawal of the written description rejection was error because purportedly: “the examiner did not analyze whether the applicants were in possession of the claimed combinations of elements that mix and match features from unrelated patent applications.”

486. The main complaint from the Petitioner for Ground 2 concerns the claim limitation about the client application using HTTP to upload such user information or global positioning information to a user data publishing website and the database and advertising. Petitioner also asserts that these two systems may be **distinct**.

487. I have reviewed Singh 129, Singh 906 and the prosecution history (and especially pages 5, 6, 8, 16, 24, and 25 ('121 Notice of Allowance) (EXHIBIT 2014). In my opinion, the record reflects the fact that the Examiner necessarily understood that the inventors had full possession of the invention as claimed.

488. The Examiner's own proposed amendments and his Notice of Allowance details demonstrate that he did not think these were two distinct mobile applications without any common base. He appears to clearly understand both the specifications, and he himself proposed the narrowing of the claim.

489. Clearly, Singh 906 provides the disclosure of the incorporated '802 application and was filed on September 19, 2007. Singh 129 provides the disclosure for the '030, '766, '381, and '121 Patents, and was filed on December 28, 2007 (only three months after Singh 906).

 US 2008/0103906A1	
(19) United States (12) Patent Application Publication (43) Pub. No.: US 2008/0103906 A1 (43) Pub. Date: May 1, 2008	
(54) ONLINE PUBLISHING OF MULTIMEDIA CONTENT	Publication Classification (51) Int. Cl. <i>G06F 17/00</i> (2006.01) <i>G06F 15/16</i> (2006.01) <i>G06Q 30/00</i> (2006.01) (52) U.S. Cl. 705/14 ; 709/206; 715/202 (57) ABSTRACT The method and system disclosed herein publishes user created multimedia content including voice, video, text, pictures, and a combination thereof on one or more publication virtual spaces, simultaneously. A client application, provided on a mobile device, creates and transfers the multimedia content to a publishing service. A protocol is provided for synchronizing user preferences of the publication virtual spaces between the client application and the publishing service. The multimedia content may be transferred as a single multimedia file, data segments, or electronic mail attachments to a back end service of the publishing service via a front end service. The back end service creates a multimedia object from the transferred multimedia content. The back end service splices targeted advertisements with the multimedia object. The multimedia object is transferred from the back end service to the front end service and then published on the publication virtual spaces chosen by the user.
(76) Inventor: Gurvinder Singh , San Francisco, CA (US) Correspondence Address: Ashok Tankha Of Counsel, Lipton, Weinberger & Husick 36 Greenleigh Drive Sewell, NJ 08080	
(21) Appl. No.: 11/901,802 (22) Filed: Sep. 19, 2007	
Related U.S. Application Data (60) Provisional application No. 60/863,090, filed on Oct. 26, 2006.	

 US 2009/0172129A1	
(19) United States (12) Patent Application Publication (43) Pub. No.: US 2009/0172129 A1 (43) Pub. Date: Jul. 2, 2009	
(54) AUTOMATIC MULTIMEDIA UPLOAD FOR PUBLISHING DATA AND MULTIMEDIA CONTENT	Publication Classification (51) Int. Cl. <i>G06F 15/16</i> (2006.01) (52) U.S. Cl. 709/217 (57) ABSTRACT Disclosed herein is 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. A client application is provided on the BT enabled mobile device. In the absence of inbuilt BT capability, a BT communication device is provided on the digital data capture device. The BT communication device is paired with the BT enabled mobile device to establish a connection. The client application detects capture of data and multimedia content on the digital data capture device and initiates transfer of the captured data, multimedia content, and associated files. The digital data capture device transfers the captured data, multimedia content, and the associated files to the client application. The client application automatically publishes the transferred data and multimedia content on one or more websites.
(75) Inventors: Gurvinder Singh , San Francisco, CA (US); Marcos Klein , Mountain View, CA (US); Vince Laviano , Alviso, CA (US) Correspondence Address: Ashok Tankha 36 Greenleigh Drive Sewell, NJ 08080	
(73) Assignee: CellSpin Soft Inc. (21) Appl. No.: 12/333,303 (22) Filed: Dec. 11, 2008	
Related U.S. Application Data (60) Provisional application No. 61/017,202, filed on Dec. 28, 2007.	

490. It is clear to me that the inventors merely added new improvements to certain Bluetooth details and incorporated the mobile client application as disclosed in Singh 906. As illustrated below, the written description in both the specifications (Singh 906 and Singh 129) is almost identical, especially with respect to mobile “client application” using “transport protocol” “HTTP”, “XML-RPC” and “user preferences.” Again, the fact that the two specifications are only 3 months apart is telling.

Singh 906 filed on Sep 19th 2007 [0047] If the user 201 is not satisfied 405 with the created multimedia object, the user 201 may review or delete 406 the multimedia object and start recording again. Otherwise, the user 201 transfers the multimedia object for publishing to a publication space selected by the user 201. Additional information such as the list of the user preferences of the publication virtual spaces 205, authentication identification, user preferences, default settings, manually entered geographical codes, and auction identifiers for eBay® and other shopping websites are selected 407 and transferred along with the user created multimedia content to the publishing service 204. A remote method call 408 such as extensible markup language-remote procedure call (XML-RPC) may be initiated by the client application 202 to transfer the user created multimedia content along with the additional information to the publishing service 204. The transfer to the nisms to achieve the connectivity between the publishing service 204 and the client application 202 is the wireless internet. While most PDAs have an inbuilt wireless network card for the internet connectivity, the mobile phones may transfer data to the publishing service 204 over the telephony network at near broadband speeds. Some of the mobile phones equipped with both wireless network and telephony data capabilities may use either of the two to communicate with the publishing service 204. The transport protocol that is used between the client application 202 and the publishing service 204 may be hypertext transfer protocol (HTTP) or extensible markup language-remote procedure calls (XML-RPC). The back end 204c service may be developed in Java. [0062] It will be readily apparent that the various methods and algorithms described herein may be implemented in a computer readable medium appropriately programmed for	Singh 129 filed on Dec 28th 2007. The client application 203 automatically publishes the transferred image on one or more websites via the internet 501. The user 502 may set preferences in the mobile device 202. The user preferences, for example, comprise the websites selected for publishing the transferred image. The user 502 may select websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc. and store the preferences on the mobile device 202. The user 502 may also set the timer setting for publishing the transferred image on the selected websites. After the captured image is transferred to the mobile device 202, the client application 203 publishes the capture image on the selected websites based on the default timer and website settings configured by the user 502 on the mobile device 202. The client application 203 may be rendered independent 30 of the operating system of the mobile device 202. One of the transport mechanisms to achieve the connectivity between the publishing service 401 and the client application 203 is the wireless internet. While most PDAs have an inbuilt wireless network card for the internet connectivity, the 35 mobile phones may transfer data to the publishing service 401 over the telephony network at near broadband speeds. Some of the mobile phones equipped with both wireless network and telephony data capabilities may use either of the two to communicate with the publishing service 401. 40 The transport protocol that is used between the client application 203 and the publishing service 401 may be hypertext transfer protocol (HTTP) or extensible markup language-remote procedure calls (XML-RPC). The back end service 401b may, for example, be developed in Java.
--	--

491. Excerpted text from Singh 906 (without Bluetooth and other details) (Publishing system **without** connected Bluetooth device) is presented below for reference:

[0018] “The client application 202 communicates the **user publishing information** including the **user preferences** of the publication virtual spaces 205 to the front end service”

[0047] “If the user 201 is not satisfied 405 with the created multimedia object, the user 201 may review or delete 406 the multimedia

object and start recording again. Otherwise, the user 201 **transfers** the **multimedia** object for publishing to a **publication** space selected by the user 201. **Additional information** such as the list of the **user preferences** of the publication virtual spaces 205, **authentication identification**, user preferences, default settings, manually entered **geographical codes**, and auction identifiers for eBay® and other shopping websites are selected 407 and **transferred along with the user created multimedia** content to the publishing service 204. A remote method call 408 such as extensible markup language-remote procedure call (**XML-RPC**) may be initiated by the client application 202 to transfer the user created multimedia content along with the additional information to the publishing service 204”

[0061] “The **transport protocol** that is used between the **client application 202** and the publishing service 204 may be **hypertext transfer protocol (HTTP)** or extensible markup language-remote procedure calls (**XML-RPC**)”

492. Similarly, excerpted text from Singh 129 (Publishing **using** connected Bluetooth device) is presented below for reference:

[8:28-8:35] “The **client application** 203 automatically **publishes the transferred image** on one or more websites via the internet 501. The user 502 may set **preferences** in the mobile device 202. The **user preferences**,

for example, comprise the web sites selected **for publishing** the transferred image. The user 502 may select websites, for example, Flickr, Picasa, YouTube, eBay(R), etc. and store the preferences on the mobile device 202.”

[9:55-9:61] “The transport protocol that is used between the **client application 203** and the publishing service 401 may be **hypertext transfer protocol (HTTP)** or extensible markup language-remote procedure calls (XML-RPC).”

[7:57-7:60] “user publishing information between the client application203 and the publishing service 401. The user publishing information may, for example, **comprise user preferences** of the websites and the timer setting.”

[9:06-9:14] “The method and system disclosed herein **enables Jane to** automatically upload pictures and videos taken using her digital camera or video camera onto a mobile device 202 and **publish the pictures**, videos, etc. from her mobile device 202 to the internet 501 with one click or touch of a button. On one click or touch of a button, the pictures and videos are published and immediately made available on **Jane’s private blog.**”

493. The side-by-side comparison clearly shows both those applications have a common system and the main difference is additional Bluetooth functionality. The written description in both the specifications (Singh 906 and

Singh 129) is almost identical, especially with respect to mobile “client application” using “transport protocol” “HTTP”, “XML-RPC” and “user preferences” “user publishing information.” This is clear to a POSITA.

494. In my opinion, the Examiners’ own Notice of Allowance shows that he not only understood the scenario but actually proposed his own amendments in the interview with the inventor. Moreover, the Amendments proposed by the Examiner included the very thing that Petitioner now claims was NOT in the original specification, namely: GPS information, which was ONLY in the incorporated reference:

Examiner Amendment

An examiner’s amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Applicant agreed that the examiner’s amendment, authorized by Ashok Tankha on 2/2/23

use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network, wherein the mobile software application is further configured to use the Hypertext Transfer Protocol to send a user preference to the remote server over the cellular data network, and wherein the user preference comprises global positioning system information; and

display a mobile advertisement inside the mobile software application;

495. It is further recognized that the '381 Patent was issued *after* the '121 Patent. As such, the Examiner was already aware of the Singh 906 incorporation from before, and he once again personally proposed the incorporation of material from Singh 906. This was after already doing the same thing two years earlier for the '121 Patent.

496. Petitioner's suggestion that the Examiner made the same alleged mistake multiple times is unsupported and contrary to the record, and runs against my understanding that Examiners are presumed to have performed their duties properly. As a POSITA, the Examiner's actions are consistent with the conclusion that he fully understood the incorporated materials.

497. I note again that the Examiner narrowed the claims by using the material from Singh 906 on two separate occasions. Likewise, the Examiner himself initiated the interview twice to narrow the claims using the Singh 906 specification. Again, it was the Examiner himself who proposed the addition of HTTP with GPS from Singh 906 into the patent claims. These facts are consistent with a full understanding and acceptance of the incorporated material.

498. In sum, it is my opinion that all of the terms in each of the Challenged Claims is adequately supported by the written description, when such is properly viewed from the perspective of a POSITA. Upon review, a POSITA would

appreciate that the inventors were in possession of the inventions as claimed, and the Examiner's actions are fully consistent with this, as well.

499. All opinions expressed in this Written Report are my own. If called upon to testify, I could and would testify in accordance with the opinions expressed herein, and as further supported and elaborated upon in the accompanying Exhibits.

VIII. SUMMARY AND CONCLUSION

500. As set forth herein, it is my opinion that none of the Challenged Claims are rendered obvious by any combination of art cited in the Petition.

501. It is my further opinion that all of the Challenged Claims are fully supported by the written description.

502. END OF WRITTEN PORTION OF REPORT