

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

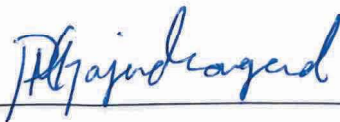
U.S. Patent No. 9,900,766 B2

IPR2024-00770

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

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

SECOND DECLARATION OF PAVAN M. GAJENDRAGAD



PAVAN M. GAJENDRAGAD
EXECUTED MAY 2, 2025

TABLE OF CONTENTS

I.	EXPERT QUALIFICATIONS AND SCOPE	1
II	INFORMATION CONSIDERED	2
III.	BRIEF SUMMARY OF OPINIONS.....	2
IV.	SUPPLEMENTAL OPINIONS.....	3
	A. MySpace.....	3
	B. Hiroishi in view of Kahn, Endsley, and Bluetooth.....	4
	1. Pairing was optional in Bluetooth as of 2007, and the Bluetooth 2.1 Specification was non-enabled prior art as of December 2007	4
	2. Authentication is NOT part of Pairing.....	10
	3. Bluetooth link NOT maintained on continuous basis	11
	4. Event Notifications are not taught by the cited art, either alone or in combination.....	14
	5. Polling for New Data is not taught.....	17
	6. Kahn does not satisfy the HTTP limitations	19
	7. Database for User Profile is not present in Kahn.....	20
	8. Bluetooth Pairing	21
	9. Kahn Bluetooth Link	22
	10. Timestamp not a “signal to notify”	24
	11. No “Listening” or “Processing of the Signal to Notify”	24
	12. Kahn is insufficient.....	25
	C. Singh ’129 in view of Singh ’906	26
	1. “Timestamp” is disclosed.....	26
	D. Claim Construction	26
	1. Along With	26
	2. Object	27
V.	SUMMARY AND CONCLUSION.....	28

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 Second Written 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 certain arguments offered by Petitioners and their expert, Dr. Patrick Traynor, 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. My understanding of the Asserted Patents, Challenged Claims, Date of Invention, Legal Framework, and Claim Construction, are all as set forth in my earlier Declaration dated January 3, 2025 (hereafter as “Gajendragad [Exhibit 2001]”). In addition, I hereby adopt the various sections of my earlier Declaration, including my earlier opinions and discussions of the relevant technologies and individual prior art references.

3. My background, including my resume, are discussed and appended to my earlier Declaration. As such, I do not repeat them again here.

4. All opinions and facts as stated in this Second 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

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

6. The Written and Supplemental Reports of Dr. Patrick Traynor, including all appendices thereto, and the papers filed by petitioners in these matters.

7. The various references as identified by Dr. Patrick Traynor in his Reports.

8. The various additional websites, sources, and documents as cited throughout my original Report, as well as those cited in this Second Written Report.

9. The Court's Claim Construction procedures and status as have been explained to me by counsel.

10. The Asserted Patents and their related file histories.

III. BRIEF SUMMARY OF OPINIONS

11. Based on my experience and training, and based on my personal analysis of the various alleged prior art references cited by Dr. Patrick Traynor and

the Asserted Claims, as well as the other documents and things as cited or referenced in this Second 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 Petitioners and Dr. Patrick Traynor. Moreover, it is my opinion (in direct contrast to the opinions of Dr. Patrick Traynor) that the various alleged prior art references and their combinations fail to teach many of the elements of the Asserted Claims, and in certain cases the proposed combinations actually lead to “unworkable” solutions, when compared with the inventions as claimed in the Asserted Claims. A POSITA would have had NO reasonable expectation of success in implementing the combination

IV. SUPPLEMENTAL OPINIONS

12. I have read the entirety of Dr. Patrick Traynor’s Supplemental Written Report, as well as the Reply prepared by Petitioners. In addition to the opinions expressed in my original Report, I offer the following supplemental opinions.

A. MySpace

13. In my opinion, as of 2007, MySpace was the biggest social network in the world during that general timeframe. Certainly, a POSITA would be highly motivated and inclined to rely upon the definition used by MySpace for “user profile,” which was also partnering with other sources at the time.

B. Hiroishi in view of Kahn, Endsley, and Bluetooth
1. Pairing was optional in Bluetooth as of 2007, and the Bluetooth 2.1 Specification was non-enabled prior art as of December 2007

14. I am aware of no evidence showing that *any* device had actually implemented or enabled the relevant portions of the Bluetooth 2.1 Specification before the December 2007 priority date. This is unsurprising, since no such devices existed. *See* Exhibit 2023 (available at: www.bluetooth.org/bluez-21-devices/).

15. The Bluetooth 2.1 Specification was released in July 2007, yet as of August 2008, “no Bluetooth 2.1 device made it to market.” While some devices had Bluetooth 2.1 capable chips in August 2008, the host stacks still ran Bluetooth 2.0, meaning manufacturers had not yet implemented Secure Simple Pairing features. *See* Exhibit 2023. Even the most expensive phone released in July 2008 (the iPhone 3G), only supported Bluetooth 2.0 with EDR – not Bluetooth 2.1. *See* Exhibit 2024 (available at: <https://everymac.com/systems/apple/iphone/iphone-faq/iphone-bluetooth-support-by-model.html>); *see also* Exhibit 2025 (available at: www.gsmarena.com/apple_iphone_3g-2424.php).

16. The text in the Bluetooth 2.1 Specification for Security Mode 4 (TTI-1019, 1273, 1286) actually says as follows:

When both devices support Secure Simple Pairing, GAP shall default to requiring an unauthenticated link key and enabling encryption.

17. In Bluetooth there are many types of pairings: Secure Simple Pairing, Simple Pairing, LMP-Pairing, and Pairing. Not only is pairing optional, the type of pairing is also itself optional. See TTI 1019, page 10, 20, 25, 26:

5 Secure Simple Pairing Overview 57 5.1 Security Goals 57 5.2 Passive Eavesdropping Protection 57 5.3 Man-In-The-Middle Protection 58 5.4 Association Models 59 26 July 2007 10	11 Appendix B (Informative): Information Flows of Related Procedures 240 11.1 LMP-authentication 240 11.2 LMP-pairing 241 11.3 Service discovery 242 12 References 243 Part D TEST SUPPORT Contents 247 1 Test Methodology 249 1.1 Test Scenarios 249 1.2 References 256 2 Test Control Interface (TCI) 259 26 July 2007 26
Part C GENERIC ACCESS PROFILE Contents 171 Foreword 175 1 Introduction 176 1.1 Scope 176 1.2 Symbols and conventions 176 2 Profile overview 178 2.1 Profile stack 178 2.2 Configurations and roles 178 2.3 User requirements and scenarios 179 2.4 Profile fundamentals 180 2.5 Conformance 180 3 User interface aspects 181 3.1 The user interface level 181 3.2 Representation of Bluetooth parameters 181 3.3 Pairing 184 4 Modes 185 4.1 Discoverability modes 185 26 July 2007 25	7 Simple Pairing Sample Data 810 7.1 P-192 Sample Data 810 7.2 Hash Functions Sample Data 811 8 Whitening Sequence Sample Data 821 9 FEC Sample Data 824 10 Encryption Key Sample Data 825 10.1 Four Tests of E1 825 10.2 Four Tests of E21 830 10.3 Three Tests of E22 832 10.4 Tests of E22 With Pin Augmenting 834 10.5 Four Tests of E3 844 26 July 2007 20

18. Neither Pairing or Secure Simple Pairing is a default in Bluetooth 2.1, and I see no evidence for how or why a POSITA would select any of them. Again, the focus of Petitioner seems to be on Secure Simple Paring, without recognizing that there are many kinds of pairing in the Bluetooth 2.1 Specification.

19. The conditional “when” (above) means that there are cases where both devices do NOT support Secure Simple Pairing, and there is no showing that any device in Hiroshi, Kahn, Takahashi, Endsley, and/or Fineberg supported Secure Simple Pairing (or even Pairing). Indeed, none of the words “pairing,”

“pair,” or “paired” even exist in Hiroshi, Kahn, Takahashi, Endsley, and/or Fineberg. Even today it is a well-known fact that NOT all Bluetooth devices or chips support Secure Simple Pairing or Pairing, because there are number of use cases that don’t require it (*e.g.*, field sensors (temperature, location, pressure), advertising beacons, Bluetooth broadcasting, toys, etc.).

20. The phrase “shall default” (above) is calling for “unauthenticated” and only encryption, and that too only for Secure Simple Pairing, not every kind of pairing.

21. Petitioner’s Reply identifies “prevention of eavesdropping, as a motivation to perform Secure Simple Pairing.” However, the prevention of eavesdropping can be readily achieved by just enabling encryption. As such, the additional step of Secure Simple Pairing is not reasonable or required.

22. Even the US NIST recommendation document that came out almost one year after the priority date ONLY calls for using Security Mode 4 and the “shall default” in Security Mode 4 is still “unauthenticated.” To the extent NIST is considered at all, NIST is only calling for a Security Mode 4 “shall default” to encryption – NOT Authentication, Authorization, or Pairing.

23. None of the terms “pairing,” “pair,” or “paired” appear in Hiroshi, Kahn, Takahashi, Endsley, and/or Fineberg, and I see no evidence that any of their connections are Paired.

24. In its Reply, Petitioner asserts that there was no battery drain issue with Bluetooth because the “pairing process need only happen once for each pair of devices,” yet Petitioner has no answer for why the Bluetooth standards body had to come up with a Bluetooth Low Energy model after the 2.1 version.

25. While it is, of course, correct that initial pairing and exchange of link keys is only done once, devices using Bluetooth 2.1 had to expend a lot of battery energy to make sure if the paired devices are still in range (distance), reachable (interference, walls, metals), and measure signal strength (that can lead to longer reconnection times). Hence the battery drain.

26. Bluetooth devices utilize a process called signal strength detection to determine if a paired device is still within range. This is done by measuring the Bluetooth Received Signal Strength Indicator (RSSI). The RSSI reflects the strength of the signal received at the receiver's end, allowing devices to estimate the distance between them. If the signal strength falls below a certain threshold, the devices understand that the other is no longer within range and can disconnect.

27. Constant RSSI Measurements are performed to check signal strength and distance of paired devices. When a Bluetooth device is paired with another, it periodically checks the strength of the radio signal coming from the paired device at the baseband level. The constant checking of RSSI values from paired devices is needed to figure out if and when they are out of range. Constant checking is also

needed for automatic reconnection when the devices move back within range. This constant RSSI measuring and checking for paired devices keeps going whether the paired devices are in range or out of range. In view of the foregoing, the act of Pairing in Bluetooth 2.1 is NOT a one-time event. Rather, pairing consumes power constantly because of constant RSSI checks that drain the battery. In fact, TTI-1019, 202, 327, 764, 813, and 1308 say as follows:

202: “It is done by measuring RSSI and reporting back if the transmission power shall be increased or decreased if possible.”

327: “the RSSI value of the inquiry response message shall be measured. It shall keep probing at different hop channels and in between listening for response packets”

764: “The RSSI measurement compares the received signal power with two thresh old levels, which define the Golden Receive Power Range.”

813: “The Inquiry Result with RSSI event indicates that a Bluetooth device or multiple Bluetooth devices have responded so far during the current Inquiry process.”

1308 “The TX Power Level tag may be used to calculate path loss on a received EIR packet using the following equation: $\text{pathloss} = \text{Tx Power Level} - \text{EIR_RSSI}$ ”

8.1.5 TX Power Level

The TX Power Level tag indicates the transmitted power level of the EIR packet.

Value	Description
0x0A	TX Power Level (1 byte) 0xXX:-127 to +127dBm Note: when the TX Power Level tag is not present, the TX power level of the EIR packet is unknown.

The TX Power Level tag may be used to calculate path loss on a received EIR packet using the following equation:

$$\text{pathloss} = \text{Tx Power Level} - \text{EIR_RSSI}$$

For example, if Tx Power Level = +4 (dBm) and the RSSI on the EIR packet is -60 (dBm) then the total pathloss is $+4 - (-60) = +64$ dB. If a second EIR packet were received at -40dBm with a Tx Power Level tag = +15dBm the resulting pathloss would be +55dB. An application could use these pathloss values to choose which device it thinks might be closer (the one with the lower pathloss value).

Unfortunately, due to fading and varying antenna, circuit, and chip characteristics, these resulting pathloss values will have uncertainty. Some of the uncertainty (for example, due to fading) may be able to be removed if multiple EIR packets are received from the same device.

8.1.6 Secure Simple Pairing Out of Band (OOB)

An out of band mechanism may be used in Secure Simple Pairing to communicate discovery information as well as other information related to the pairing

26 July 2007

Extended Inquiry Response Data Format

1308

28. Petitioner wrongly asserts that in its Reply that: “Mr. Gajendragad acknowledged at his deposition that his knowledge of pairing was limited” (citing to TTI-1039, 17:8-21:8). This is a clear overstatement, as I endeavored to diligently answer all questions while occasionally noting that the proper response “depends on the implementation” (because it obviously does). Likewise, I stated that “I have to consult the spec” to be sure of certain aspects, since the Bluetooth Specification is a 1400-page document. In offering my responses to questions during my deposition, I made every effort to be precise.

2. Authentication is NOT part of Pairing

29. Authentication is different from Pairing, and Pairing does not always mean Authentication is present. Moreover, both are optional.

30. Petitioner's new theory on Authentication seems to be based on using only Secure Simple Pairing. The Reply brief section header says: "Authentication Is Part of Secure Simple Pairing," yet Petitioner fails to realize that in Bluetooth there are many types of pairings: Secure Simple Pairing, Simple Pairing, LMP-Pairing and Pairing. Again, all those are different options and kinds of Pairing in Bluetooth. Not only is pairing OPTIONAL, to opt for what kind of pairing to implement is also optional. This is reflected below (*see* TTI 1019, page 10, 20, 25, 26). Petitioner never advances any theory as to how or why a POSITA would only use Secure Simple Pairing. To reiterate, neither Pairing or Secure Simple Pairing was a default in Bluetooth 2.1, and Petitioner has not shown otherwise.

5	Secure Simple Pairing Overview	57
5.1	Security Goals	57
5.2	Passive Eavesdropping Protection	57
5.3	Man-In-The-Middle Protection	58
5.4	Association Models	59

26 July 2007

10

Part C	
GENERIC ACCESS PROFILE	
Contents	171
Foreword	175
1 Introduction	176
1.1 Scope	176
1.2 Symbols and conventions	176
2 Profile overview	178
2.1 Profile stack	178
2.2 Configurations and roles	178
2.3 User requirements and scenarios	179
2.4 Profile fundamentals	180
2.5 Conformance	180
3 User interface aspects	181
3.1 The user interface level	181
3.2 Representation of Bluetooth parameters	181
3.3 Pairing	184
4 Modes	185
4.1 Discoverability modes	185

26 July 2007

25

11	Appendix B (Informative): Information Flows of Related Procedures	240
11.1	LMP-authentication	240
11.2	LMP-pairing	241
11.3	Service discovery	242
12	References	243

Part D	
TEST SUPPORT	
Contents	247
1 Test Methodology	249
1.1 Test Scenarios	249
1.2 References	258
2 Test Control Interface (TCI)	259

26 July 2007

26

7	Simple Pairing Sample Data	810
7.1	P-192 Sample Data	810
7.2	Hash Functions Sample Data	811
8	Whitening Sequence Sample Data	821
9	FEC Sample Data	824
10	Encryption Key Sample Data	825
10.1	Four Tests of E1	825
10.2	Four Tests of E21	830
10.3	Three Tests of E22	832
10.4	Tests of E22 With Pin Augmenting	834
10.5	Four Tests of E3	844

26 July 2007

20

3. Bluetooth link NOT maintained on continuous basis

31. Petitioner for the first time in its Reply argues: “Hiroishi maintains its Bluetooth connection on a continuous basis.” This is a new theory and new assertion not present anywhere in the original Petition. In any event, Petitioner’s new theory is factually wrong.

32. The known FACT is in Bluetooth 2.1 and before, connections (paired or otherwise) were NOT maintained on a continuous basis at ALL. Indeed, Bluetooth 2.1 relies on the connection interval and link supervision timeout to maintain the link connection for a specified amount of time. This was done for many reasons but one of them being the high drain on the battery on the phones with continuous connection for Bluetooth 2.1 and before.

33. Link Supervision Timeout defines how long the Bluetooth device will wait for a response from the other Bluetooth device before assuming the connection is disconnected. The default timeout setting for disconnection in Bluetooth 2.1 (if there is no data from the other device) is 20 seconds. See TTI-1019 page 578:

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2]		page 408 of 906
Host Controller Interface Functional Specification		 Bluetooth
6.20 LINK SUPERVISION TIMEOUT		
The Link_Supervision_Timeout parameter is used by the master or slave Bluetooth device to monitor link loss. <u>If, for any reason, no Baseband packets are received from that Connection Handle for a duration longer than the Link_Supervision_Timeout, the connection is disconnected.</u> The same timeout value is used for both synchronous and ACL connections for the device specified by the Connection Handle. Note: Setting the Link_Supervision_Timeout to No Link_Supervision_Timeout (0x0000) will disable the Link_Supervision_Timeout check for the specified Connection Handle. This makes it unnecessary for the master of the piconet to unpark and then park each Bluetooth Device every ~40 seconds. By using the No Link_Supervision_Timeout setting, the scalability of the Park state is not limited.		
Value	Parameter Description	
0x0000	No Link_Supervision_Timeout.	
N = 0xFFFF	Size: 2 Octets Range: 0x0001 to 0xFFFF Default: 0x7D00 Mandatory Range: 0x0190 to 0xFFFF Time = N * 0.625 msec Time Range: 0.625 msec to 40.9 sec Time Default: 20 sec	

34. The remote control of Hiroshi, even if it implemented Bluetooth 2.1 (which it was not) would NOT maintain paired connection on a continuous basis. The connection would disconnect after 20 seconds of inactivity as a default and a maximum of 40.9 seconds. The assertions to the contrary by Petitioner and its

expert are simply wrong, and do not reflect an understanding of basic Bluetooth 2.1 functionality.

35. “Connection Interval” (Hold Mode Max Interval, Sniff Mode Max Interval and all the others) determines how often a connection data exchange occurs, and is expressed in multiples of 1.25ms. A shorter interval means more frequent data exchange but also increased power consumption. See TTI-1019 page 646, 648 (below). But it is ALWAYS less than the link supervision timeout.

The Hold_Mode_Max_Interval shall be less than the Link Supervision Timeout configuration parameter.	
Command Parameters:	
<u>Connection_Handle:</u>	Size: 2 Octets (12 Bits meaningful)
Value	Parameter Description
0xXXXX	Connection Handle to be used to identify a connection. Range: 0x0000-0x0EFF (0x0F00 - 0x0FFF Reserved for future use)
<u>Hold_Mode_Max_Interval:</u>	Size: 2 Octets
Value	Parameter Description
N = 0xXXXX	Maximum acceptable number of Baseband slots to wait in Hold Mode. Time Length of the Hold = $N * 0.625$ msec (1 Baseband slot) Range for N: 0x0002-0xFFFE; only even values are valid. <u>Time Range: 1.25ms - 40.9 sec</u> Mandatory Range: 0x0014 to 0x8000

Command Parameters:	
<u>Connection_Handle:</u>	Size: 2 Octets (12 Bits meaningful)
Value	Parameter Description
0xXXXX	Connection Handle to be used to identify a connection. Range: 0x0000-0x0EFF (0x0F00 - 0x0FFF Reserved for future use)
<u>Sniff_Max_Interval:</u>	Size: 2 Octets
Value	Parameter Description
N = 0xXXXX	Range: 0x0002 to 0xFFFE; only even values are valid Mandatory Range: 0x0006 to 0x0540 Time = $N * 0.625$ msec <u>Time Range: 1.25 msec to 40.9 sec</u>

36. A POSITA, when combining Hiroshi with Bluetooth 2.1, would certainly not make it continuous because the battery on the phone and the camera would not last more than 2 hours. There is no motivation to keep the continuous connection and would make the solution inoperable for most practical applications. When the POSITA uses the default standard Bluetooth 2.1, the POSITA would have soon discovered that the connection is disconnected after no activity is detected after 20 seconds.

4. Event Notifications are not taught by the cited art, either alone or in combination

37. In IPR2024-00768, Petitioner said “event driven” would not “have been pertinent to Bluetooth” but the reality is that the industry found it pertinent and Event Notifications were introduced in Bluetooth Low Energy (BLE), which was part of Bluetooth 4.0, and was released in 2010. *See* Bluetooth 4.0 Specification, available at: www.bluetooth.com/specifications/specs/core-specification-4-0/.

38. Petitioner asserts that “even in the ‘event driven architecture,’ the component expecting an event must wait.” This statement is simply false. In the event driven architecture, the component expecting an event is passively “listening.” That means the thread is not blocked, and the component is actively doing other things, and just listening in the background (asynchronously) for an event if it occurs in next time period.

39. Applications can be designed to do nothing if the event happens, or do nothing if the event does not happen. This does not change the fact that “event driven architecture” is markedly different from “request response architecture.” There is no discussion of synchronous or asynchronous in the specification, because in 2007, the POSITA would have known that when one component is “listening” for an “event” or “signal” from another component it is common knowledge that this is based on event architecture.

40. Petitioner further argues that “nothing prevents software from sending requests and responding to events, and thus having aspects of both these alleged architectures.” While I do not necessarily disagree with that statement, it nevertheless merits mentioning that if the whole software has 50 components, each component can do its own thing. But each particular component would only do one or the other. For example, one could have three data acquiring components: one is based on request-response, the second is based on polling, the third is based on event-notification. This does not mean ALL three of them are the same. And Hiroshi and Kahn only disclose request-response.

41. Petitioner argues that since the claim has a limitation that says “request to enable event notifications,” somehow event notification is request-based. This is incorrect, as requests to enable event notifications once do not make the event-based systems a request-based system. Enablement for the event

notification is only done once for plurality of events and there is NO subsequent request to get “each” event notification. Once enabled, the event notifications keep on getting generated every time there is new-data. There is no individual request for each new signal/event notification. A POSITA understands that you have to “enable” event notifications once. There is NO request to “get” notifications.

42. For these reasons, a POSITA would never think that Hiroshi or Kahn are teaching any event notification, enabling event notification, listening for event notification, or processing event notifications. The Petitioner misapplies basic computer science coding differentiation between event-based-notification-listening and basic request-response mechanisms.

43. Still further, Petitioner asserts: “Hiroshi specifically discloses the transmission of image data containing multiple thumbnails.” Of course, it is noted that sending a request to the camera of Hiroshi to send all images or 12 images that have already been captured previously, is not the same as enabling event notifications once, to send a new notification every time a new image is captured on the camera. The point is that in Hiroshi, every time a photo is to be received, the Hiroshi state machine has to send a request. Conversely, the patents call for the enablement of event notifications, and after the event notifications are enabled, there is NO need to send any other request to get the newly captured photo. The event architecture will automatically send the event signal when the camera

captures the new image/data. There is NO need for subsequent request messages for new images. The event-based architecture is completely different.

44. In summary, event architecture is different from request-response and is different from polling. These terms cannot be conflated, which is what Petitioner does repeatedly.

5. Polling for New Data is not taught

45. I am informed that the claim construction agreed by Petitioner at the District Court for “poll / polling” is: “checking status [of] on a predetermined basis.”

46. In its Reply, Petitioner again asserts that this “limitation is met by Hiroshi’s request for thumbnails,” with no evidence of checking status [thumbnail] on a predetermined basis anywhere in Hiroshi.

47. Further, Petitioner originally relied on Bluetooth specification (TTI-1019, 332) in support of its contention that “Bluetooth teaches polling.” *See, e.g.*, TTI 1019, 332 (8.6.1 Polling in the active mode). Specifically, Bluetooth teaches that “to avoid collisions on the ACL logical transport.” Hiroshi’s “request for thumbnail” is NOT checking status on a predetermined basis of anything. Rather, it is a simple request for thumbnail.

48. Petitioner’s Reply now only relies on Bluetooth 2.1 specification and its “T poll Slots.” Specifically, Petitioner says: “For example, see the ‘Polling in

the active mode' section where a 'master normally attempts to poll a slave ... no less often than once every T_{poll} slots.' TTI-1019, 332."

49. The reliance on T poll slots is factually wrong. "T poll" in Bluetooth 2.1 is used to "support bandwidth allocation and latency control," it is a QoS (quality of service) metric for the piconet connections to avoid collisions at the data link layer level (link manager protocol) when there are multiple slaves and has NOTHING to do with new data captured or thumbnails or any higher-level data. See TTI-1019, 404:

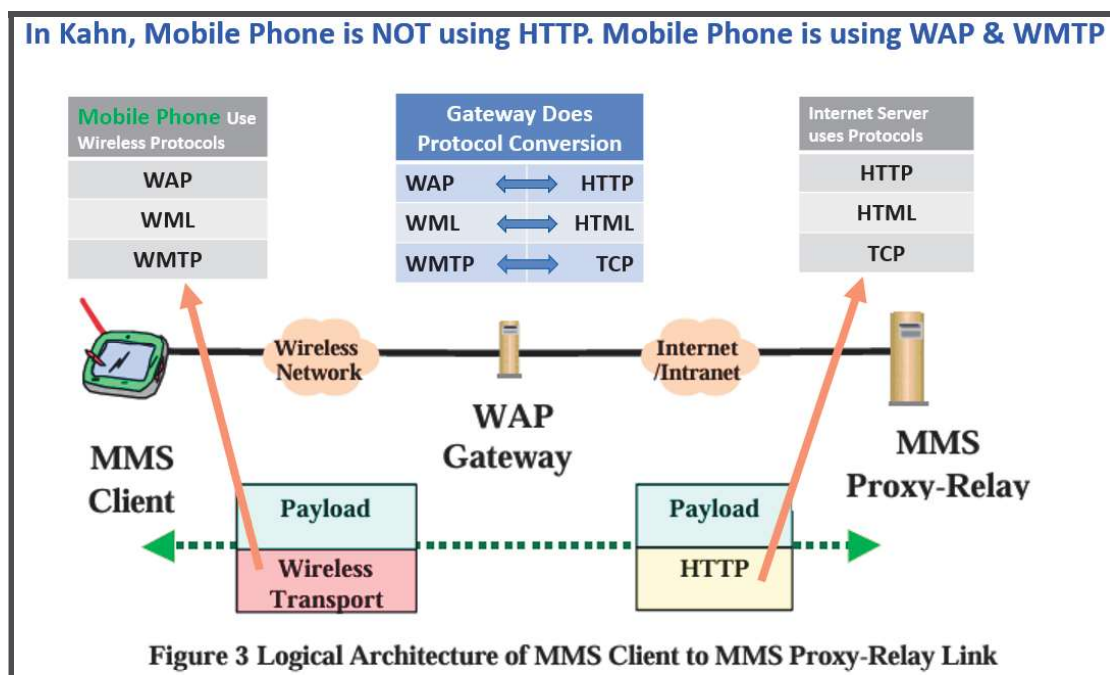
BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2]	page 234 of 906
<u>Link Manager Protocol</u>	
4.1.8 Quality of service (QoS)	
The LM provides QoS capabilities. A <u>poll interval, T_{poll}, that is defined as the maximum time between transmissions from the master to a particular slave on the ACL logical transport, is used to support bandwidth allocation and latency control</u> - see Baseband Specification, Section 8.6.1, on page 162 for details. <u>The poll interval is guaranteed in the active and sniff modes except when there are collisions with page, page scan, inquiry and inquiry scan, during time critical LMP sequences in the current piconet and any other piconets in which the</u>	

50. T Poll is mainly used for avoiding collisions when there are more than one slaves in a Piconet, in one-to-one connections they are not even used. See TTI-1019, 332.

51. Clearly, a POSITA would not combine low level T poll that is used as a QoS metric at the "link manager protocol" in Bluetooth 2.1 to the mobile application of the Hiroshi thumbnail request.

6. Kahn does not satisfy the HTTP limitations

52. In Kahn, the use of gateway illustrates that Mobile phone is NOT using HTTP, even if the image server uses HTTP. The claim requires the mobile software to use HTTP for upload, not WAP and not WMTP. In the WAP gateway scenario, the mobile phone will use WAP and not HTTP. The WAP gateway will do the translation. The claims, on the other hand, require the mobile device to use HTTP and NOT WAP, WML, WMTP, or WSL. Below, I provide an annotated version of the image relied on by Petitioner to showcase what protocols are used where and how the translation works on the WAP Gateway. Support for this WAP to HTTP translation can be found in Exhibit 2026 (2006 Cisco IOS WAP Gateway document, at page 2 figure 1) (The non-annotated base image is from page 15 of TTI 1013):



7. Database for User Profile is not present in Kahn

53. Petitioner mis-states the teachings of the cited art. Specifically, Petitioner claims: “Kahn teaches that the image manager database is keyed to the user ID, location ID, and other information associated with user. TTI-1017, [0098].” Of course, the actual text says: “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). The location information that is associated with the images is not necessarily permanent.”

54. The database is keyed by image ID and the database “includes” fields for user ID, timestamp and location ID. Clearly, data is NOT keyed by timestamp or location or user ID – these are fields in the database table. The follow-on text makes it even more clear that the included location field (not key) can be changed: “the user may re-ID the images with another location, as desired.” That means that in this image database location field of the image-123xyz could be changed from Paris to Venice. There is NO user profile or even User ID database. Rather, Kahn only has “Image database” that has location, timestamp and user id as fields, and is only keyed by Image ID.

55. Petitioner argues that: “a POSITA reading Kahn would have recognized that the User Account tab, coupled with the databased keyed to user ID and location ID would have satisfied” the user profile limitation. Of course, there

are several factual problems with this theory. First, this theory was not present in the Original Petition. Second, having a web page UI for a phone company that says “account” does not mean the backend has a user profile database. There is no evidence in Kahn that this account info was coming from a database, and if this database had just the phone number and monthly bill due and other fees. Even that is pure speculation at best, because Kahn does not show what the account info page looks like in the prior art. Third, Petitioner again falsely claims that the database is keyed to User ID, which it is not – it is only keyed to image ID.

56. Not Used

57. Not Used

58. Not Used

8. Bluetooth Pairing

59. There are many types of pairings in Bluetooth: Secure Simple Pairing, Simple Pairing, LMP-Pairing, and Pairing. Not only is pairing OPTIONAL, to opt for what kind of pairing, is also optional. As shown below (TTI 1019, page 10, 20, 25, 26), neither Pairing or Secure Simple Pairing is a default in Bluetooth 2.1.

5	Secure Simple Pairing Overview	57
5.1	Security Goals	57
5.2	Passive Eavesdropping Protection	57
5.3	Man-In-The-Middle Protection	58
5.4	Association Models	59

20 July 2007

10

11	Appendix B (Informative): Information Flows of Related Procedures	240
11.1	LMP-authentication	240
11.2	LMP-pairing	241
11.3	Service discovery	242
12	References	243

Part D
TEST SUPPORT

Contents	247
1 Test Methodology	249
1.1 Test Scenarios	249
1.2 References	258
2 Test Control Interface (TCI)	259

26 July 2007

26

Part C
GENERIC ACCESS PROFILE

Contents	171
Foreword	175
1 Introduction	176
1.1 Scope	176
1.2 Symbols and conventions	176
2 Profile overview	178
2.1 Profile stack	178
2.2 Configurations and roles	178
2.3 User requirements and scenarios	179
2.4 Profile fundamentals	180
2.5 Conformance	180
3 User interface aspects	181
3.1 The user interface level	181
3.2 Representation of Bluetooth parameters	181
3.3 Pairing	184
4 Modes	185
4.1 Discoverability modes	185

29 July 2007

25

7	Simple Pairing Sample Data	810
7.1	P-192 Sample Data	810
7.2	Hash Functions Sample Data	811
8	Whitening Sequence Sample Data	821
9	FEC Sample Data	824
10	Encryption Key Sample Data	825
10.1	Four Tests of E1	825
10.2	Four Tests of E21	830
10.3	Three Tests of E22	832
10.4	Tests of E22 With Pin Augmenting	834
10.5	Four Tests of E3	844

26 July 2007

20

60. Petitioner’s expert erroneously states (at page 16) that “unsecure communications are only present in the Bluetooth 2.1 for backward compatibility,” without any citation to the Bluetooth specification and without realizing that the optional security features were always present in Bluetooth. Moreover, Petitioner’s expert fails to realize that security and pairing are not required for the majority of everyday scenarios, which require openness with Bluetooth beacons, ad sensors, external and industrial sensors, etc.

9. Kahn Bluetooth Link

61. Petitioner argues: “In the context of the Kahn-Bluetooth combinations, a POSITA would have understood that to mean that the paired Bluetooth connection between the camera and the host device was maintained on a continuous basis.” This theory is factually wrong.

62. Kahn does not even have the word “Bluetooth” in it; thus, the purported Kahn-Bluetooth grounds rely solely on the Bluetooth specification for the Bluetooth connections. The known FACT is in Bluetooth 2.1 and before, connections (paired or otherwise) were NOT maintained on a continuous basis at ALL. Indeed, Bluetooth 2.1 relies on the connection interval and link supervision timeout to maintain the link connection for a specified amount of time. This was done for many reasons but one of them being the high drain on the battery on the phones with continuous connection for Bluetooth 2.1 and before.

63. The Bluetooth specification at the time of the inventions had a default non-continuous connection. The link supervision timeout was 20 seconds as the default, and 40.9 seconds as a maximum. The Bluetooth-Khan connection was clearly not continuous, and could not have been continuous in 2007.

64. A POSITA, when combining Kahn with Bluetooth 2.1, would certainly not make it continuous because the battery on the phone and the camera would not last more than 2 hours. There is no motivation to keep the continuous connection and would make the solution inoperable for most practical applications. In fact, Kahn has a clear recommendation (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.” Even in this text cited by Petitioner, the main recommendation for POSITA is still occasionally

connected (see Kahn [0055]): “In the currently preferred embodiment, the camera device 310 is a stand-alone unit that is occasionally (or persistently) connected to the host device 320.” The POSITA will look at the totality of the recommendation that is contrary to continuous connections, and if POSITA tried to experiment with default standard Bluetooth, the POSITA would have soon found out that the connection is disconnected after no activity is detected after 20 seconds.

10. Timestamp not a “signal to notify”

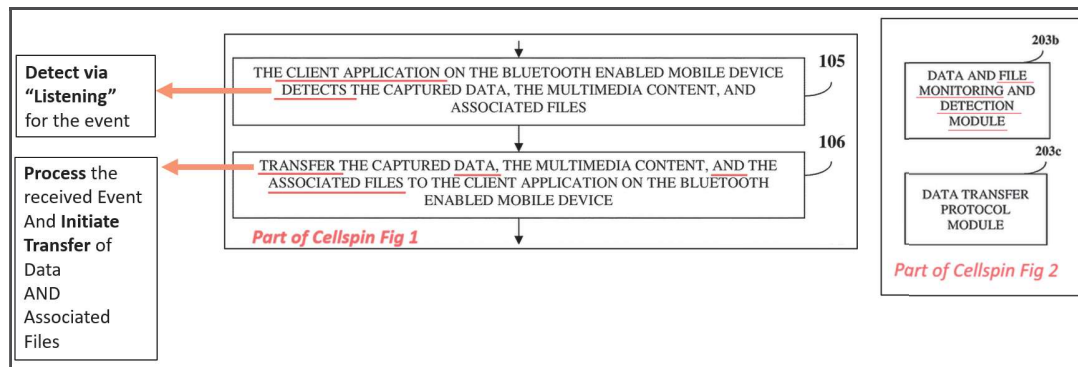
65. A “timestamp” cannot be a “signal to notify” for a variety of reasons. The claims simply do not require “re notify” or “retry” “re send” or “send it twice or 15 times.” In fact, neither the claims or the specification even suggest retrying to send the notification if it fails. A POSITA understands what “notification” means, and it does not mean “renotifying” about the same image again and again.

11. No “Listening” or “Processing of the Signal to Notify

66. Even if the Kahn “timestamp” was considered as a “signal to notify” for transfer (which it should not), Kahn is neither listening for nor processing the “time stamp” for transfer (as required by the claims). Similarly in Kahn-Feinberg, Kahn is neither listening for nor processing the “thumbnail” for transfer.

67. In my opinion, a POSITA would appreciate that the specification clearly discloses (*see* 5:20-23 of the ’847 Patent) the listening and processing the events: “A file event listener in the client application 203 listens for the signal from

the digital data capture device 201” and module 203b and 203c are doing the listening and processing of the event:



12. Kahn is insufficient

68. The claim is clear: “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.”

Petitioner suggests that the GPS in the header is not a signal for transfer. But by the same token, Kahn also plainly does not say that the additional “thumbnail” in the header is a signal for transfer, and Petitioner has not pointed to any text in Kahn or Feinberg to suggest otherwise.

69. Similarly, Kahn also does NOT say “timestamp” in the header is a signal for transfer, and Petitioner points to no evidence to the contrary.

70. If GPS is just metadata, then so too are the thumbnail and timestamp. There is NO text in Kahn or Feinberg relating them to a “signal to notify for transfer.”

C. Singh '129 in view of Singh '906

1. “Timestamp” is disclosed

71. Petitioner makes the strained argument that the multitude of instances in the specification discussing “time” and “timer” are insufficient to disclose a “timestamp” to a POSITA. I note that the word “time” is mentioned 9 times in the specification and the word “timer” is mentioned 24 times. In view of the “time” related disclosures, as well as the robust disclosures around Bluetooth OBEX (Object) usage for data transfer, the “timestamp” is readily apparent to a POSITA.

72. In the Bluetooth wireless field, “time” and “timer” convey “timestamp” to skilled artisans, and usage of OBEX conveys the necessary context.

73. Petitioner further argues between two different timestamps; namely: “last modified” and “acquired,” but in the process fails to realize that “last modified” includes the freshly acquired scenario. The last modified timestamp would be the same as acquired time stamp.

D. Claim Construction

1. Along With

74. A POSITA would not understand the term “along with” to mean: “inside.” In Takahashi, the “User ID” is embedded “inside” the filename. The User ID of Takahashi is *not* sent “in addition to” the filename, nor is it sent “together with” the file name. The claims plainly require that the User ID and File

be separate. If filename is inside the file and inside the file header structure of the file, then filename cannot be “along with”, “in addition to” or even “together with” the file, if it is already a part of the file data inside and being part of the file header data.

75. The context in the '802 disclosure is very clear to a POSITA that all the things envisioned by the patentee to be sent “along with” cannot be “inside” the file name.

76. In Takahashi, the User ID is part of the file data, since it is embedded in the file name, whereas the claims require the file and User ID to be two different things.

2. Object

77. The Microsoft 2006 document clearly says that, even in MTP, the Object is different from a File. Still further, in MTP, “object” has three (3) separate components (*see* TTI-1040, 18):

MTP object consists of not only the binary content of the file, but also the descriptive metadata and references.

In MTP, an object is the combination of the binary file, its descriptive metadata and any intra-object references.

78. It is abundantly clear to POSITA that even in MTP, there are different definitions for “file” and “object.”

79. Further, it is clear that with “Object Push” you can push both small data and file. But with “File Push” you can only send files, not small amount of data, encapsulated as an object. Hence “Object Push” and “File Push” are different. More importantly, for an “Object Push” to send the file, the file is first converted to an Object.

80. Petitioner further states that the value “file data” in the file is either “referenced” or is an “intra-object references” by the “filename” inside the file header as required by MTP definition. This assertion is incorrect. For example, there is zero evidence that says any file format (*e.g.* RFC of JPEG or RFC of PNG) uses “filename” as a “reference” or a “intra-object references” (pointer) to “file data” in the “file header.” There is NO file type where “file-data” is referenced (or is considered “intra-object references”) by a filename in the file header.

V. SUMMARY AND CONCLUSION

81. 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.

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

83. 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.

84. END OF WRITTEN PORTION OF REPORT